Titre: Title:	Routage intégré dynamique et hybride avec support de la qualité de service pour réseaux GMPLS à haut débit
Auteur: Author:	Nabil Harrabida
Date:	2005
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Harrabida, N. (2005). Routage intégré dynamique et hybride avec support de la qualité de service pour réseaux GMPLS à haut débit [Master's thesis, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/8416/

UNIVERSITÉ DE MONTRÉAL

ROUTAGE INTÉGRÉ DYNAMIQUE ET HYBRIDE AVEC SUPPORT DE LA QUALITÉ DE SERVICE POUR RÉSEAUX GMPLS À HAUT DÉBIT

NABIL HARRABIDA
DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
SEPTEMBRE 2005

Your file Votre référence
ISBN: 978-0-494-47668-0
Our file Notre référence
ISBN: 978-0-494-47668-0

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

ROUTAGE INTÉGRÉ DYNAMIQUE ET HYBRIDE AVEC SUPPORT DE LA QUALITÉ DE SERVICE POUR RÉSEAUX GMPLS À HAUT DÉBIT

Présenté par : HARRABIDA Nabil

En vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées

A été dûment accepté par le jury d'examen constitué de :

M. CHAMBERLAND Steven, Ph.D., président

M. PIERRE Samuel, Ph.D., membre et directeur de recherche

M. QUINTERO Alejandro, Doct., membre

REMERCIEMENTS

À Monsieur Samuel PIERRE,

Vous êtes à l'origine de ce travail de recherche, c'était un pari à la fois ambitieux et motivant. Votre clairvoyance et la qualité de votre encadrement ont permis de le mener à bien. J'ai grandement apprécié l'esprit professionnel et pédagogique avec lequel vous motivez l'ensemble des membres du LARIM. Pour tout cela, acceptez, Monsieur, l'expression de mes remerciements les plus sincères.

À Monsieur Steven CHAMBERLAND,

Je vous remercie de me faire l'honneur de présider le jury et vous assure mon respect et ma gratitude.

À Monsieur Alejandro QUINTERO,

Vous m'avez honoré en acceptant de participer au jury. Je vous en remercie vivement.

À Monsieur Yves LEMIEUX,

Pour votre disponibilité et la qualité de votre encadrement au sein de Ericsson Recherche, veuillez accepter, Monsieur, mes remerciements les plus chaleureux.

À mon épouse,

Pour avoir supporté mon indisponibilité et mes absences. Merci beaucoup.

RÉSUMÉ

Avec l'avènement de l'Internet pendant les dernières années et la migration du trafic temps réel et mission critique vers les réseaux IP, la survivabilité des réseaux de télécommunications est devenue un aspect très important dans la gestion des fautes. De plus, la convergence des réseaux IP et optiques avec le plan de contrôle unifié de GMPLS a fait de la résilience une exigence critique des réseaux à haut débit, puisqu'une coupure d'une fibre optique peut engendrer plusieurs pannes de liens et de nœuds au niveau des couches supérieures.

Plusieurs solutions de survavibilité ont été proposées dans le cadre des travaux de l'IETF. Ces propositions peuvent être classées en deux grandes catégories : les *techniques de protection* et les *techniques de restauration.* Les mécanismes de protection sont conçus pour réagir aux pannes d'une façon très rapide mais requièrent des fois une redondance totale des ressources réseau. Quant aux mécanismes de restauration, ils assignent dynamiquement les ressources de secours quand une panne se produit. De ce fait, elles sont moins rapides comparées aux techniques de protection, mais présentent l'avantage de moins utiliser les ressources réseau.

Une des faiblesses de ces mécanismes est qu'ils ne tiennent pas, en général, compte des différentes exigences de qualité de service et de résilience des divers types de trafics. D'autre part, ils adoptent une approche typique d'approvisionnement de LSP à savoir, assumer le modèle de réseau en couches (*overlay*) dans lequel chaque couche réseau est traitée comme une entité séparée avec son propre plan de contrôle. La couche IP/MPLS n'a aucune connaissance des ressources disponibles dans les couches inférieures. Ainsi, le choix des LSPs primaires et de protection est fait sans prendre en considération les possibilités de protection déjà disponibles à la couche inférieure, ce qui résulte en une mauvaise utilisation des ressources réseau.

L'objectif de notre travail de recherche est de concevoir un algorithme de routage avec contraintes (constraint-based routing algorithm) permettant à la fois de définir et les chemins primaires et ceux de secours. Le domaine d'application de cet

algorithme serait les réseaux GMPLS à haut débit, avec des exigences de qualité de service des réseaux dorsaux présents dans l'infrastructure des opérateurs de réseaux cellulaires.

Nous avons proposé un algorithme de routage dynamique et intégré permettant le choix des LSPs (Label Switched Path) primaires et de secours. Ce nouvel algorithme tire profit du plan unifié de GMPLS en prenant en considération les ressources réseau en termes de protection optique et de disponibilité de bande passante. De plus, le mécanisme de protection est adaptatif aux exigences de résilience de chacune des classes de trafic transportées. Afin d'évaluer les performances de notre proposition, nous l'avons comparée par simulation avec le protocole de routage CSPF. Nous avons considéré la probabilité de panne du LSP primaire et le taux d'utilisation des ressources de protection, comme métriques de comparaison. Notre approche présente de meilleurs résultats que le protocole CSPF et permet d'établir des LSPs résilients tout en optimisant l'utilisation des ressources de protection.

ABSTRACT

With the advent of the Internet during last years and the migration of real-time and high-priority traffics to IP networks, the survivability of telecommunication networks became a very important aspect in fault management. Moreover the resilience becomes more important than ever before in high capacity networks where the IP and optical networks have converged with a GMPLS-based control plane. Indeed, the resilience turns to be a vital aspect of the current and future high capacity networks based on the GMPLS control plane since a single cut of an optical fiber may generate several link and node failures in higher layers.

Several survivability mechanisms have been proposed within the IETF. These proposals can be classified in two main categories: *Protection techniques* and *Restoration techniques*. The protection mechanisms are designed to react to the failure in a very fast way but require sometimes a total redundancy of the network's resources. As for the mechanisms of restoration, they assign the resources of recovery dynamically when a failure occurs. So they are slower compared with the protection techniques, but have the advantage of using less network's resources.

One of the weaknesses of these mechanisms is that they don't take into account the different classes of traffic in a network. In addition, they adopt a typical provisioning approach, by assuming an overlay model, in which each network layer is treated as an independent entity with its own control plane. The IP/MPLS layer is not aware of the resources available in the sub-layers. Thus, the choice of the primary and backup LSPs is made without taking into account the possibilities of protection already available at the sub-layers, which results in a misuse of the network resources.

The objective of our research is to design a constraint-based routing algorithm to route primary LSPs and their backups. The algorithm will be applied to a GMPLS high speed backbone network. We proposed a dynamic and integrated routing algorithm allowing the choice of primary LSPs and their backups. This new algorithm benefits from the GMPLS' unified control plane, by taking into account the optical protection

and the available bandwidth on the links. Moreover, the protection mechanism is adaptive to the resilience requirements of each class of traffic. In order to evaluate the performance of our solution, we compared it by simulation with CSPF protocol. We considered the failure probability of the primary LSP and the utilization ratio of the protection resources, as comparison's metrics. Our approach offers better results than CSPF protocol and makes it possible to establish resilient LSPs while optimizing the protection-resources usage.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTES DES TABLEAUX

LISTE DES SIGLES ET ABRÉVIATIONS

ATM	Asynchronous Transfer Mode
CR-LDP	Constrained Routing – Label Distribution Protocol
CSPF	Constrained Shortest Path First
DHIRQ	Dynamic Hybrid Intergrated Routing with Quality of Service
DiffServ	Differentiated Services
EF	Expedited Forwarding
FEC	Forwarding Equivalence Class
FIS	Failure Indication Signal
FRS	Failure Recovery Signal
GMPLS	Generalized Multi-Protocol Label Switching
IETF	Internet Engineering Task Force
IP	Internet Protocol
IS-IS	Intermediate System-to-Intermediate System
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LSP	Label Switched Path
LSR	Label Switch Router
MP	Merge Point
MPLS	Multi-Protocol Label Switching
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PLR	Point of Local Repair
PML	Path Merge LSR
PSL	Path Switch LSR
QoS	Quality of Service

RC	Resilience Class
RSVP-TE	Resource Reservation Protocol Traffic Engineering
SONET	Synchronous Optical Network
TCP	Transmission Control Protocol
TE	Traffic Engineering
TOS	Type of Service
UDP	User Datagram Protocol

CHAPITRE I
INTRODUCTION

L'avènement de l'Internet au cours des dernières années a fait que la technologie des réseaux de télécommunications a dû s'adapter constamment à de nouvelles demandes accrues de bande passante. De plus, on vit une aire de *convergence* où les trafics données, voix et vidéo sont tous transportés sur le même réseau. Cette convergence apporte de nouveaux défis qui sont intrinsèques à la nature des trafics temps réel tel que la voix et la vidéo, mais aussi qui découlent de la nécessité pour les réseaux d'assurer une certaine qualité de service selon le trafic transporté. Plusieurs technologies ont été proposées pour satisfaire ces nouvelles contraintes. Les protocoles MPLS et son extension GMPLS paraissent actuellement comme une option intéressante étant donné qu'ils combinent la rapidité des commutateurs de la couche 2 et l'intelligence des routeurs de la couche 3, tout en assurant la convergence des réseaux IP et des réseaux optiques dans le cas de GMPLS. Un des aspects importants qui est inhérent aux réseaux à haut débit (MPLS/GMPLS) est la gestion des pannes pouvant survenir aux liens et/ou nœuds constituant le réseau. D'où l'importance de développer de nouvelles techniques assurant une meilleure *survivabilité* avec un faible coût en terme de temps et de ressources, ce qui constitue l'objet de ce mémoire. Dans ce chapitre d'introduction, nous allons d'abord définir les concepts de base nécessaires à la compréhension des éléments de la problématique, puis nous préciserons nos objectifs de recherche, pour finalement esquisser le plan du mémoire.

1.1 Concepts de base

Dans les réseaux typiques non orientés connexion tel qu'Internet, la transmission de paquets est exécutée indépendamment à chaque routeur dans le réseau et est basée sur l'adresse de destination contenue dans le paquet. Récemment, des efforts considérables ont été faits pour faire évoluer l'architecture et les protocoles conventionnels de routage IP, en les enrichissant avec de nouvelles fonctionnalités et extensions dans le cadre des

travaux de développement du protocole MPLS, et dernièrement du protocole GMPLS qui constitue une extension de MPLS pour le support de types de transmission autres que la transmission par paquet. Une application de MPLS/GMPLS est le routage par contrainte (constraint-based routing), qui est utilisé pour calculer les chemins qui répondent à diverses exigences sujets à un ensemble de contraintes. Le routage par contrainte est utilisé à deux fins principales dans les réseaux contemporains: *l'ingénierie du trafic* (traffic engineering) et le *re-routage rapide* (fast reroute). Un des mérites du protocole MPLS, c'est qu'il permet l'élimination des couches réseau superflues en transférant certaines des fonctions fournies par des couches ATM et SONET/SDH vers le plan de contrôle IP/MPLS.

Des travaux récents (Mannie, 2003; Kompella et Rekhter, 2002; Berger, 2003) ont été effectués pour étendre et adapter le plan de contrôle de MPLS, et spécifiquement le routage par contraintes, de sorte qu'ils puissent être employés pas simplement avec des routeurs et des commutateurs ATM, mais également avec les cross-connects optiques (OXCs). C'est une étape fondamentale dans la convergence des réseaux IP et des architectures de réseau optiques. En utilisant MPLS comme base pour l'établissement de connexions et comme un plan commun de contrôle, cela permet d'adresser plusieurs problèmes liés à l'évolution des réseaux. En effet, l'adoption d'un seul plan de contrôle simplifie les opérations et la gestion de réseau, qui a finalement comme conséquence la réduction des coûts opérationnels. De plus, développer un plan de contrôle commun en réutilisant et en améliorant des protocoles existants de routage et de signalisation évite le besoin de « réinventer la roue » et réduit les risques liés au développement de nouveaux protocoles.

Comme pour toute nouvelle technologie, plusieurs néologismes ont été créés pour décrire les dispositifs qui constituent l'architecture MPLS/GMPLS. On retrouve ainsi les éléments suivants : les LSR, les LSP, les étiquettes, les nœuds Ingress et Egress, et les FEC. Le *routeur commutateur d'étiquettes* ou LSR (*Label Switch Router*) implémente les procédures de distribution d'étiquettes et peut transmettre des paquets en fonction des étiquettes. Un *chemin commuté d'étiquettes*, ou LSP (*Label Switched Path*)

consiste pour l'essentiel en une description de l'ensemble des LSRs qu'un paquet étiquetté doit traverser pour atteindre le *LSR egress* correspondant à une classe FEC déterminée. Le nœud ou LSR Ingress est un LSR qui se charge d'encapsuler et d'ajouter une étiquette aux paquets reçus en provenance d'un domaine autre que celui auquel appartient le LSR Ingress. Le routeur Egress est le LSR qui se situe à la frontière du domaine MPLS/GMPLS et qui se charge de transmettre les paquets d'un LSP du domaine MPLS/GMPLS au domaine IP. L'imposition ou l'affectation d'étiquette à un paquet est une fonction de périphérie, ce qui signifie que les paquets sont étiquetés avant d'être transmis dans le domaine MPLS par les nœuds Ingress. Une classe d'équivalence de transmission ou FEC (*Forwarding Equivalence Class*) est l'ensemble de paquets qui doivent recevoir un traitement identique entre le nœud Ingress et le nœud Egress. La classe FEC attribuée au paquet est ensuite encodée sous la forme d'un petit identificateur appelé *étiquette.*

1.2 Eléments de la problématique

Pendant que le réseau Internet s'est développé exponentiellement au cours des dernières années, la majeure partie du trafic sur ce réseau continue d'être transmise en se basant sur le protocole IP (Internet Protocol) qui, à cause de sa conception originelle, souffre de manque de support de la qualité de service. En effet, le protocole IP est basé sur une technique de routage "meilleur effort" (*best effort*), ce qui en d'autres mots signifie absence de garantie en terme de délais de bout en bout. Les équipements réseau essaient de transmettre le trafic à la destination en utilisant les informations de routage et les ressources réseau disponibles. Si le réseau échoue à transmettre le trafic, à cause d'un manque d'information de routage ou de ressources, les paquets sont tout simplement rejetés. Cette approche n'est pas adéquate aux réseaux IP actuels et spécialement aux trafics temps réel tel que la voix et la vidéo qui requièrent une garantie de qualité de service.

MPLS et son extension GMPLS sont les technologies les plus prometteuses pour faire face aux problèmes traditionnels d'IP et pour répondre aux exigences des nouvelles

applications réseaux. Une des importantes exigences des réseaux actuels est la *survivabilité*. Plusieurs propositions ont été faites dans le cadre des travaux de l'IETF. Ces propositions peuvent être classées en deux grandes catégories : les *techniques de protection* et les *techniques de restauration*. Les mécanismes de protection sont conçus pour réagir aux pannes d'une façon très rapide mais requièrent des fois une redondance totale des ressources réseau. Quant aux mécanismes de restauration, ils assignent dynamiquement les ressources de secours quand une panne se produit. De ce fait, elles sont moins rapides comparées aux techniques de protection, mais présentent l'avantage de moins utiliser les ressources réseau.

Dans le cas de la protection, on distingue deux techniques : la *protection locale* ou reroutage rapide et la *protection globale* ou protection par commutation. Avec la *protection locale*, le recouvrement commence au point de détection de la panne. Cette méthode est transparente au nœud source (Ingress). Dans le cas de la protection globale, le nœud d'entrée (Ingress) prend la responsabilité du rétablissement de chemin après réception du signal d'indication de défaut (*Fault Indication Signal* FIS). Cette méthode exige l'établissement d'un chemin de secours disjoint du chemin principal.

Dans le cas de la restauration, deux variantes sont disponibles : la restauration *pré-planifiée de LSP,* aussi désignée sous le nom de re-routage pré-planifié de LSP, et la *restauration de LSP,* aussi désignée sous le nom de re-routage de LSP. Pour la *restauration pre-planifiée,* avant la détection et/ou la notification de panne, un ou plusieurs LSPs de secours sont instanciés entre la même paire de nœuds du LSP. L'établissement complet de la restauration LSP se produit seulement après la détection et/ou la notification de la panne. Quant à la *restauration de LSP*, elle consiste à ce que le nœud d'entrée (ingress) commute le trafic normal sur un LSP alternatif de secours signalé et entièrement établi après la détection de la panne.

Une des faiblesses de ces mécanismes est qu'ils ne tiennent pas compte des différentes exigences de qualité de service et de résilience des divers types de trafics. D'autre part, ils adoptent une approche typique d'approvisionnement de LSP à savoir, assumer le modèle de réseau en couches (*overlay*) dans lequel chaque couche réseau est

traitée comme une entité séparée avec son propre plan de contrôle. La couche IP/MPLS n'a aucune connaissance des ressources disponibles dans les couches inférieures. Ainsi, le choix des LSPs primaires et de protection est fait sans prendre en considération les possibilités de protection déjà disponibles à la couche inférieure, ce qui résulte en une sous-utilisation des ressources réseau. Ce mémoire s'inscrit donc dans le cadre de travaux de recherche visant à développer un mécanisme qui permettra une utilisation efficace des ressources réseau et assurera une résilience adéquate selon la qualité de service exigée, en tirant profit du plan de contrôle unifié de GMPLS, où les informations de topologie, de disponibilité des ressources et des mécanismes de protection sont connus et partagés par l'ensemble des couches.

1.3 Objectifs de recherche

L'objectif principal de ce mémoire est de concevoir un algorithme de routage avec contrainte (*constraint-based routing algorithm*) permettant à la fois de définir et les chemins primaires et ceux de secours, tout en respectant un ensemble de critères de Qualité de Service (QdS). Le domaine d'application de cet algorithme serait les réseaux GMPLS à haut débit, avec des exigences de qualité de service des réseaux dorsaux présents dans l'infrastructure des opérateurs de réseaux cellulaires. De manière plus spécifique, nous visons à :

- analyser les algorithmes et techniques de résilience identifiés dans la littérature ;
- concevoir et implémenter un algorithme hybride (Protection locale et globale) de routage avec les contraintes intrinsèques aux réseaux avec convergence voix et données ;
- évaluer la performance de l'algorithme proposé en le comparant avec le protocole de routage CSPF dans OPNET.

1.4 Plan du mémoire

Faisant suite au chapitre I d'introduction, le chapitre II présente d'abord les protocoles MPLS et GMPLS ainsi que l'état de l'art en matière de survivabilité des réseaux. Le chapitre III présente un nouvel algorithme de routage et de choix des chemins alternés basé sur la qualité de service et sur la classe des trafics transportés; il expose en détail l'approche proposée, les améliorations escomptées ainsi que la modélisation de la proposition. Le chapitre IV expose les résultats de tests et d'évaluation de performance qui seront analysés par la suite. Le chapitre V fait une synthèse des résultats obtenus et esquisse des orientations de recherche futures.

CHAPITRE II
GESTION DES PANNES ET SURVIVABILITÉ DANS LES RÉSEAUX MPLS/GMPLS

L'augmentation exponentielle des utilisateurs d'Internet et l'utilisation de plus en plus fréquente des applications multimédia et temps réel émergentes basées sur les services de télécommunication ont poussé à ce que les réseaux informatiques d'aujourd'hui transportent des capacités de données énormes croissant continuellement. Ces réseaux transportent ainsi, des trafics de plusieurs types: mission critique, haute priorité ou temps réel. Dans ce contexte de réseaux à haute capacité avec exigence de qualité de service, la survivabilité devient très critique étant donné qu'une panne de lien ou de nœud peut causer énormément de dégât (perte de données, échec de connexion...). En général, un réseau est considéré survivable s'il offre la capacité d'effectuer ses fonctions même en présence de panne sur un composant. La survivabilité peut être obtenue en mettant en oeuvre *la restauration* et/ou *la protection.* En cas de panne, la restauration recherche dynamiquement des chemins alternatifs. Les mécanismes de protection, quant à eux, réservent en avance les chemins de secours. De nombreux travaux de normalisation et de recherche ont été consacrés à la survivabilité dans les réseaux MPLS (Multiprotocol Label Switching) et récemment à son extension GMPLS (Generalized MPLS). L'ensemble des ces travaux tend à réduire l'impact des pannes sur le fonctionnement normal du réseau et ceci de différentes façons tout en ayant comme objectif commun de réduire le temps nécessaire au rétablissement et réduire la perte des données suite aux pannes. Dans ce chapitre, nous faisons une synthèse sur les mécanismes de survivabilité dans les protocoles MPLS et GMPLS. Nous présenterons d'abord les protocoles MPLS/GMPLS et la classification des mécanismes de survivabilité. Ensuite, on fera un survol des travaux de recherche et propositions présents dans la littérature.

2.1 Le Protocole MPLS

MPLS (Multiprotocol Label Switching) (Rosen et al., 2001) est une technologie destinée à répondre à plusieurs des problèmes liés à la transmission des paquets dans les réseaux IP. MPLS associe les avantages de la transmission de paquets fondée sur la commutation de la couche 2 avec ceux du routage de la couche 3 du modèle OSI. Cette architecture est divisée en deux composants distincts : le plan de transmission (data plane) et le plan de contrôle (control plane) (Davie et Rekhter, 2000). La Figure 2.1 illustre les composants d'une telle architecture. Pour réaliser la transmission des paquets de données en fonction des étiquettes qu'ils transportent, le plan de transmission se sert d'une base de données de transmission d'étiquettes maintenue par un commutateur d'étiquettes. Le plan de contrôle est chargé de la création et de la maintenance des informations de transmission des étiquettes pour un groupe de commutateurs interconnectés. En effet, le plan de contrôle a deux fonctions principales: la *découverte* et *la signalisation* des chemins.

- *Découverte de chemin (routage)* : implique la création des tables de routage

  Le protocole de routage échange l'information sur la topologie et les ressources réseau avec d'autres nœuds pour construire et maintenir une table de routage, en utilisant les protocoles de routage du niveau 3 standards, tels que OSPF (Moy, 1998) ou IS-IS (Oran, 1990).

- *Signalisation des chemins.* : La table de transmission des étiquettes (Forwarding table) est maintenue par le plan de contrôle et est distribuée aux nœuds de réseau en utilisant un protocole de signalisation, tel que le protocole de réservation de ressource (RSVP) (Braden et al., 1997) (Awduche et al., 2001) ou le protocole de distribution d'étiquette (LDP) (Andersson et al., 2001).

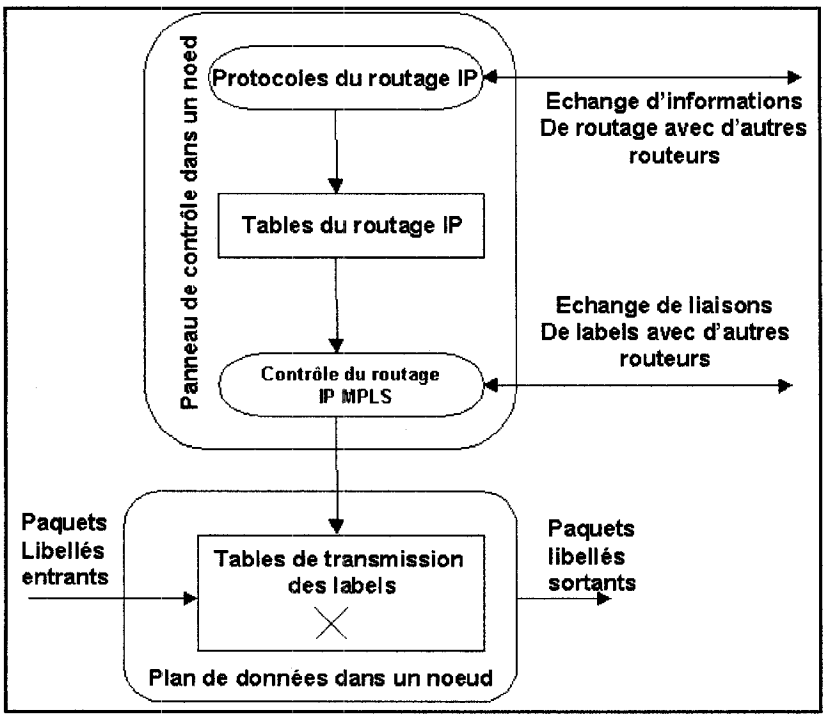

Figure 2.1 Architecture de base d'un nœud MPLS

Les extensions aux protocoles de routage OSPF et IS-IS, proposées dans le cadre des travaux de l'IETF, permettent à des nœuds d'échanger des informations sur la topologie de réseau et la disponibilité des ressources. Ces informations sont utilisées par les protocoles de routage et de signalisation tel que RSVP-TE, et CR-LDP, afin de calculer et d'établir des chemins respectant les contraintes de ressources et/ou de politique de gestion du réseau. Ceci permet à MPLS d'accomplir, d'une façon appropriée, deux buts principaux: Technologie du trafic (traffic engineering) et le reroutage rapide (fast rerouting).

2.2 Le protocole GMPLS

GMPLS (Mannie, 2003) est une extension à la technologie MPLS pour supporter des équipements de commutation non paquet (*nonpacket-switching devices*) par

exemple, les équipements de commutation basée sur le multiplexage temporel ou les longueurs d'onde. Le paradigme GMPLS est établi autour du concept clef de MPLS consistant à séparer le plan de contrôle du plan de transmission des données. Dans GMPLS, ceci a été étendu pour permettre aux messages de signalisation et de contrôle (control messages) d'être transmis sur un lien physique différent de celui utilisé pour le plan de transmission des données. Les extensions de signalisation de GMPLS étendent la notion d'étiquette *(label)* de MPLS pour inclure des intervalles de temps (time slots), des longueurs d'onde et des ports. GMPLS supporte le concept de LSP hiérarchiques tout en exigeant qu'un LSP commence et se termine sur une interface du même type. La Figure 2.2 présente la hiérarchie des LSPs ainsi que les types d'interfaces dans GMPLS.

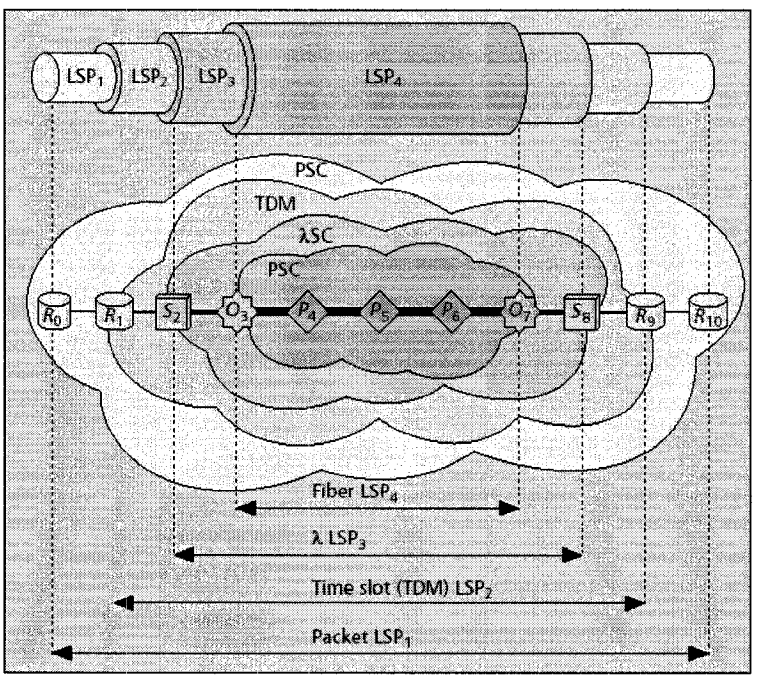

Figure 2.2 Interfaces GMPLS et LSP hiérarchiques

Les extensions apportées par GMPLS, en terme de protocole et d'objets de signalisation sont multiples, dans cette section on essaiera de mettre l'accent sur les nouveautés de GMPLS qui permettent d'assurer la protection et la restauration. Dans ce cadre on peut citer les points suivants :

Extensions au protocole RSVP-TE

Les extensions au protocole RSVP-TE (Berger, 2003) qui ont un rapport avec la gestion des pannes dans un réseau GMPLS, sont le message de notification (*Notify message*), le redémarrage du plan de contrôle après une panne (*Graceful restart/control state recovery*) et le type de protection des liens (*Link Protection*).

- *Notify message* : bien qu'efficace, la notification d'erreur de RSVP basée sur des messages de PathErr/ResvErr est lente. Ceci est dû au fait que tous les nœuds le long du chemin doivent traiter les messages de PathErr/ResvErr. En outre, si la panne affecte plusieurs LSPs en même temps, les messages multiples de PathErr/ResvErr pourraient congestionner le réseau. Le *notify message* de GMPLS est envoyé directement du point de détection de la panne au point de réparation (Point of Repair - PoR), sans être traité par les nœuds intermédiaires. Afin de réduire la charge dans le plan de contrôle, le *Notify Message* est défini de sorte qu'il puisse signaler des pannes/erreurs sur des LSPs multiples aussi longtemps que le code de la panne est le même et que l'ensemble des LSPs ont le même point de réparation .
- *Graceful restart/control state recovery* : puisque le plan de contrôle GMPLS pourrait être physiquement différent du plan de transmission des données, un mécanisme de résilience est nécessaire pour assurer le fonctionnement du plan de transmission des données même si le plan de contrôle est hors service. Pour cela, GMPLS dispose de l'objet 'Restart_cap'. Cet objet spécifie les possibilités dont dispose un nœud pour récupérer des états de GMPLS après une panne ou une remise en marche du plan de contrôle.
- *Link Protection* : un nouvel objet de protection de lien a été également ajouté pour spécifier les attributs de protection de lien. Les options pour ce champ incluent : *Amélioré*, *dédié 1+1*, *dédié 1:1*, *partagé M:N*, *non protégé* et *trafic extra*.

Extensions aux Protocoles de routage

Les extensions de OSPF-TE et IS-IS-TE (Kompella et Rekhter, 2002) permettent d'annoncer la disponibilité des ressources optiques dans le réseau et le type de protection des liens. Ces attributs sont essentiels pour l'établissement des mécanismes de protection et de restauration des chemins.

Link Management Protocol

LMP (Lang, 2003) assure la gestion du canal de contrôle (Control channel management), la vérification de la connectivité du lien (link connectivity verification), la corrélation des propriétés du lien (link property correlation) et l'isolation des pannes (fault isolation). Pour la localisation de la panne le message *ChannelStatus* est échangé. Ce message peut être envoyé sans demande au nœud adjacent pour indiquer l'état actuel du lien. Pour la localisation des pannes, un nœud en aval qui détecte une panne, envoie un message *Channel Status* au nœud adjacent en amont indiquant qu'une panne a été détectée, comme le montre la Figure 2.3.

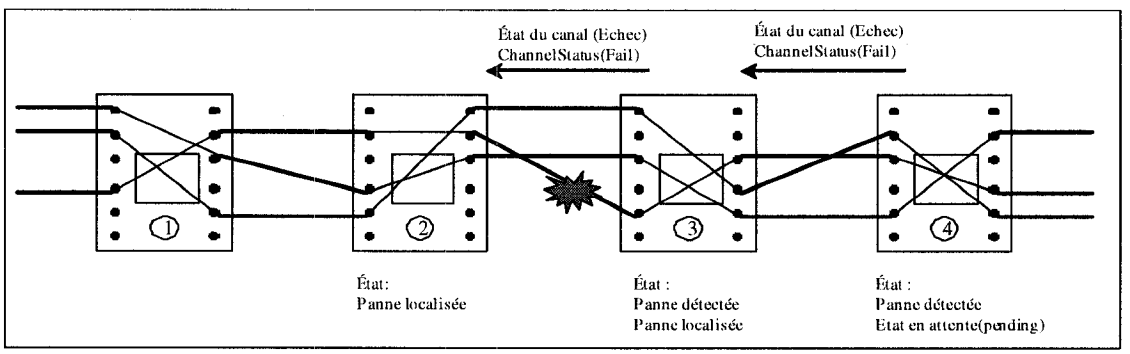

Figure 2.3 Localisation des pannes avec LMP

2.3 Classification des méthodes de recouvrement des pannes

Dans la littérature, plusieurs manières de classifier les techniques de protection et de restauration ont été présentées. Deux approches de classification seront détaillées

dans cette section : le modèle M:N et la classification basée sur l'allocation des ressources.

2.3.1 Le modèle M:N

Dans ce modèle, *M* spécifie le nombre de LSPs de secours employés pour protéger *N* LSPs primaires. Dans cette catégorie de classification, on peut citer les techniques suivantes:

- *1:1* : un LSP primaire est protégé par un LSP de secours.
- *1+1*: dans ce modèle le trafic est envoyé simultanément sur le LSP primaire et celui de secours. C'est la meilleure technique de protection au point de vue temps de rétablissement de service après une panne. Elle présente cependant l'inconvénient de consommer énormément de ressources réseau et exige un support au niveau de la technologie de la couche physique.
- *M:1* : un LSP primaire protégé par *M* LSPs de secours.
- *1:N* : *N* LSPs primaires utilisent un seul LSP de secours.

On note ici que le cas particulier de 0:1 représente une absence de protection (Best effort traffic).

2.3.2 Classification par allocation des ressources et établissement du chemin de secours

Le critère de classification ici est l'ordre chronologique dans lequel se fait le calcul du chemin de secours, sa réservation et son établissement. On distingue deux grandes catégories : *les mécanismes de protection* et *les mécanismes de restauration.*

Les mécanismes de protection sont conçus pour réagir aux pannes d'une façon très rapide mais requièrent des fois, une redondance totale des ressources réseau. Quant à eux, les mécanismes de restauration assignent dynamiquement les ressources de secours quand une panne se produit. Pour cela, elles sont moins rapides comparées aux techniques de protection, mais présentent l'avantage de moins utiliser les ressources

réseau. La Figure 2.4 illustre les différentes variantes des mécanismes de protection et de restauration classifiées par réservation des ressources et établissement des LSPs.

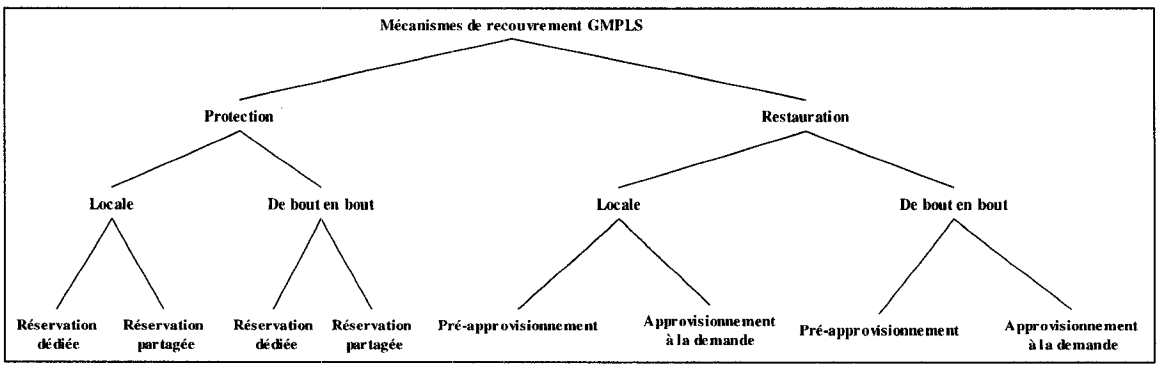

Figure 2.4 Les mécanismes de recouvrement GMPLS

La distinction principale que nous faisons entre la protection et la restauration est que les techniques de protection pré-allouent des ressources tandis que les ressources de restauration sont établies après la panne. Une question se pose pour ce qui est de l'utilisation des chemins de secours dans le cas des ressources pre-allouées. Sharma et Crane (2003) suggèrent deux options : *ressources dédiées* (*Dedicated-resources*) et *trafic extra permis* (*Extra-traffic-allowed*).

- *Ressources dédiées*: les ressources du chemin de secours sont dédiées exclusivement au transport du trafic du chemin principal et ne peuvent être utilisées pour le transport d'un autre trafic.
- *Trafic extra permis*: on permet de transporter du trafic de type extra sur le chemin de secours en l'absence de panne sur le chemin principal. On désigne par trafic extra tout type de trafic, de moindre importance, qui peut être supprimé sans enfreindre les engagements de services (Service Level Agreement SLA).

2.3.3 Classification des mécanismes de protection dans GMPLS

GMPLS définit six différents types de protection (Berger, 2003) : *amélioré*, *dédié 1+1*, *dédié 1:1*, *partagé 1:N*, *non protégé* et *trafic extra* (extra traffic).

- *Amélioré* : Ce type exige une protection fortement fiable au niveau optique tel que le BLSR/4.
- *Dédié 1+1* : Une connexion séparée est établie, et le trafic est transmis simultanément sur les connexions primaires et de protection. La destination choisit l'une des deux connexions pour la réception. En cas de panne, la destination commute simplement de la connexion principale à la connexion de protection. Ce type de protection est très rapide parce qu'aucun protocole de signalisation n'est exigé entre la source et la destination.
- *Dédié 1:1* : une connexion séparée est également établie, mais le trafic est transmis au-dessus de la connexion primaire seulement. Lors d'une panne, la source commute le trafic sur la connexion de protection.
- *Partagé 1:N* : la connexion de protection peut également être mise en partage entre plusieurs connexions primaires s'il n'est pas probable que deux connexions primaires tombent en panne en même temps. Ceci étend la protection de *1:1* à un type plus général qui est la protection *1:N*, où *N* connexions primaires, partagent un seul chemin de secours. Les deux types de *1:1* et de protection *1:N* ne sont pas aussi rapides que le *1+1 dédié* parce qu'ils exigent un échange de signalisation entre les nœuds source et destination afin de commuter le trafic sur le chemin de secours. Cependant, ils sont efficaces du point de vue capacité, parce que la connexion de protection peut être utilisée pour transmettre le trafic de basse priorité.
- *non protégé* : aucune connexion de secours n'est réservée. En cas de panne, les connexions affectées se basent sur la découverte dynamique d'un nouveau chemin. Cette découverte est réalisée au niveau IP. Ce type de protection souffre de la lenteur connue des protocoles de découverte dynamique de la couche IP. Cependant, il consomme moins de largeur de bande puisque la largeur de bande de secours n'est pas pré-allouée.

Le Tableau 2.1 récapitule les avantages et les inconvénients de chaque type de protection, en termes de capacité exigée de vitesse de commutation de protection de quantité du trafic supplémentaire qu'elle peut supporter, et de la complexité de la technique.

Tableau 2.1 Classification des mécanismes de protection dans GMPLS

Type de protection	Capacité allouée requise	Vitesse de Protection	Quantité du trafic supplémentaire pouvant être supporté	Complexité
Dédié 1+1	La plus haute	La plus rapide	Aucun	Requiert un support hardware
Dédié 1 :1	Moyenne – haute	Moyenne	Plus	Requiert un mécanisme de signalisation
Partage 1 : N	Moyenne basse	Moyenne	Moins	Requiert un mécanisme de signalisation
Non protégé	La plus basse	La plus lente	aucun	Faible- best effort
Extra trafic	Aucune	N/A	N/A	Faible

2.3.4 Classification des mécanismes de restauration dans GMPLS

Cette section présente un ensemble de techniques de restauration des LSPs. Les techniques pré-planifiées ainsi que les techniques dynamiques sont explicitées (Mannie et al., 2004).

- **Restauration pré-planifiée de LSP :** aussi désignée sous le nom de reroutage pre-planifié de LSP. Avant la détection et/ou la notification de panne, un ou plusieurs LSPs de secours sont instanciés entre la même paire de nœuds du LSP primaire. Notons ici que les LSPs de secours ne sont pas interconnectés au niveau optique (cross-connected) avant la panne. De ce fait ils ne peuvent transporter des trafics de moindre priorité (extra-traffic). L'établissement complet du LSP de secours, se produit seulement après la

détection et/ou la notification de la panne. Cette technique ressemble à la protection dédiée 1 :1, à la différence qu'avec la restauration pré-planifiée le LSP de secours ne véhicule pas de trafic en l'absence de panne.

- **Restauration de LSP :** aussi désignée sous le nom de re-routage de LSP, elle consiste à ce que le nœud d'entrée (ingress) commute le trafic sur un LSP de secours, signalé et entièrement établi après la détection de la panne. Le calcul du LSP de secours peut être fait après détection de la panne. Dans ce cas-ci, on parle d'un re-routage complet du LSP ce qui signifie que toutes les étapes d'établissement du LSP se font après la panne.

Le Tableau 2.2 récapitule les différentes variantes d'implémentation de la restauration d'un LSP. Cela dépend du choix que l'on fait quant au calcul du chemin, à la réservation des ressources et à l'assignation des canaux avant ou après la panne (Lei et al., 2003).

Tableau 2.2 Variantes d'implémentation de la restauration de LSP

Catégorie	**Fonctions**			
	Calcul du chemin	Réservation des ressources	Assignation du canal	Connexion Optique (Cross-Connect)
Restauration pré planifiée de LSP	Avant	Avant	Avant	Après
Restauration de LSP Variante 1	Avant	Avant	Après	Après
Restauration de LSP Variante 2	Avant	Après	Après	Après
Restauration complète (Full LSP Re-routing)	Après	Après	Après	Après

2.4 Mécanismes de survivabilité MPLS/GMPLS

Dans cette section nous présentons les principaux travaux de recherche ayant traité de la survivabilité dans les réseaux MPLS et GMPLS.

2.4.1 La survivabilité multicouches

Demeester et Autenrieth (1999) ont étudié la survivabilité dans les réseaux de transport multicouches. Ils ont donné des directives pour la coordination des actions de rétablissement dans les couches WDM, SONET et ATM. Papadimitriou et Jones (2002) ont étendu le concept de la coordination entre couches aux réseaux de type paquet sur un media optique (packet-over-optical). Fumagalli et Valcarenghi (2000) ont également envisagé la coopération entre la couche IP et les couches optiques afin de fournir la résilience aux réseaux. Ils ont proposé une heuristique (simulated annealing) pour choisir la configuration optimale de protection et/ou de restauration pour chaque lien du réseau. Aussi, les conditions pratiques pour la survivabilité multicouches ont été examinées dans le RFC 3386, dans lequel l'utilisation de temporisateurs (*hold-off timers*) a été recommandée. *Hold-off time* correspond au temps d'attente entre la détection de la panne et la prise en charge du recouvrement par les couches de haut niveau, afin d'accorder le temps aux couches inférieures de réparer la panne. Par exemple, le *Hold-off time* dans le cas de MPLS avec SONET peut être mis à 50 ms afin que le mécanisme de protection de SONET puisse être activé avant celui de IP/MPLS.

2.4.2 Les principaux modèles de recouvrement dans MPLS/GMPLS

Dans cette section, les principaux modèles de recouvrement des pannes sont présentés. Ces modèles ont été définis pour des réseaux MPLS dans (Huang et Sharma, 2002) et (Sharma et Crane, 2003). Certains de ces modèles ont été adaptés aux réseaux optiques dans le cas de GMPLS.

Modèle global ou centralisé

Dans ce modèle (Huang et Sharma, 2002), le nœud d'entrée (Ingress) prend la responsabilité du rétablissement de chemin après réception du signal d'indication de la panne (Fault Indication Signal FIS). Cette méthode exige l'établissement d'un chemin de secours disjoint du chemin principal. Dans ce modèle la protection est toujours activée au nœud source, indépendamment du lien qui est en panne. Ceci implique de propager la notification de panne au nœud source avant que le mécanisme de protection soit activé. Cette méthode a l'avantage d'établir un seul chemin de secours par chemin primaire.

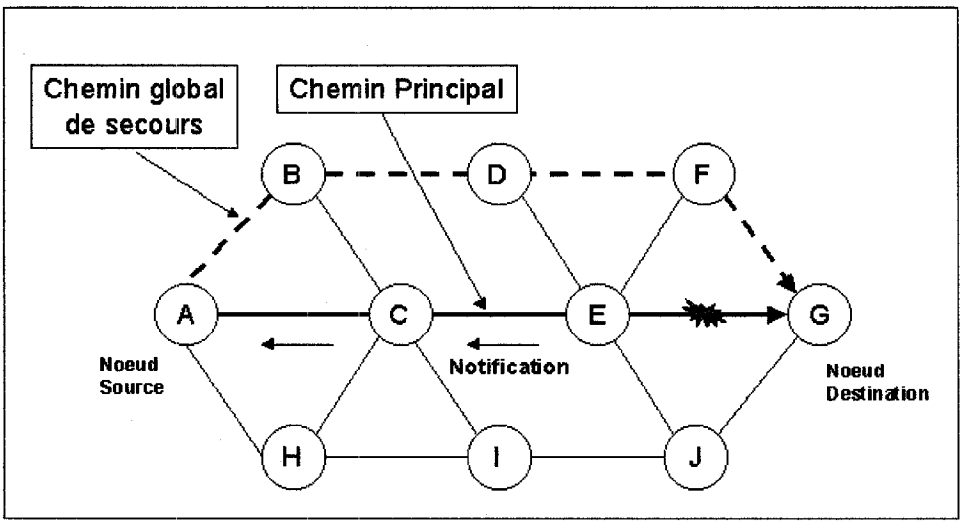

Figure 2.5 Protection globale

La Figure 2.5 montre un scénario simple constitué par dix LSRs où un chemin primaire (*A-C-E-G*) et un chemin de secours (*A-B-D-F-G*) sont pré-établis. Dans l'état normal, le trafic du nœud *A* au nœud *G*, emprunte le LSP primaire. Quand un défaut de lien est détecté (par exemple entre les nœuds *E* et *G*) un signal de notification de panne est envoyé au nœud source *A*. Quand la notification est reçue par le nœud *A*, le trafic est commuté au chemin de secours global de LSP.

Modèle de chemin inverse

La fonction principale de cette méthode est de rediriger le trafic vers le nœud source (ingress) à la suite d'une panne sur le chemin primaire. Ceci permet d'éviter la perte de paquets dont souffre la méthode globale présentée dans la section précédente. Le nœud source est responsable de commuter le trafic sur le chemin de secours et de réorienter le trafic qui lui parvient du chemin inverse. Dès que le signal de notification de panne arrive au nœud d'entrée ce dernier cesse d'envoyer le trafic au chemin primaire et commute le trafic au chemin alternatif.

Cette méthode est particulièrement appropriée dans des scénarios de réseau où les trafics sont très sensibles aux pertes de paquets. Cependant, cette méthode présente l'inconvénient de mal utiliser les ressources réseau du fait qu'on etablit deux LSPs afin d'assurer la prise en charge de la panne.

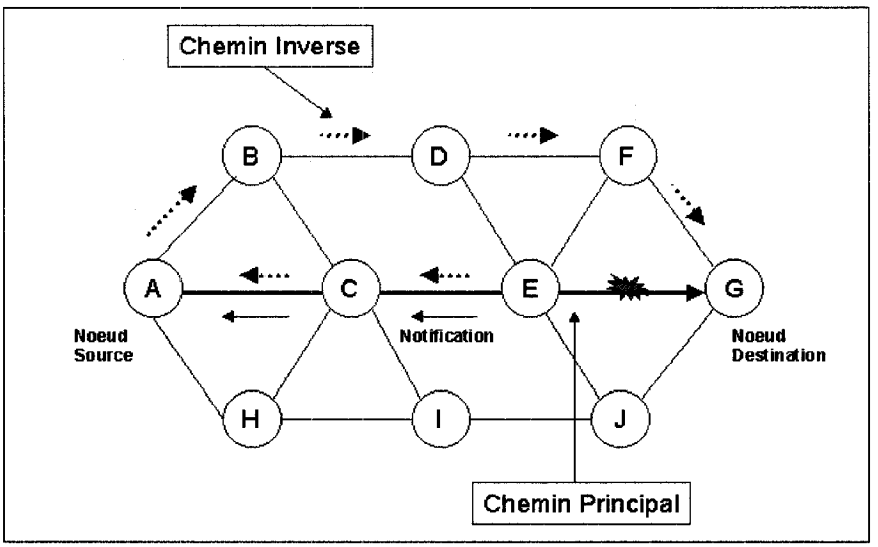

Figure 2.6 Modèle de chemin inverse

La Figure 2.6, montre un exemple d'utilisation de chemin de secours inverse. Un LSP primaire ainsi qu'un de secours sont établis comme dans le modèle centralisé. En Plus, on établit un LSP entre les nœuds *E* et *A* passant par le nœud *C*. Quand un échec de lien est détecté sur le LSP primaire entre les nœuds *E* et *G*, le trafic est commuté de

nouveau au noeud *A* en empruntant le LSP inverse (*E-C-A*), et puis commuté sur le LSP de secours comme dans le modèle centralisé.

Protection locale

Dans cette approche, le recouvrement commence au point de la panne. C'est une méthode locale qui est transparente au nœud source (Ingress). L'avantage principal de ce modèle est qu'il offre un temps de rétablissement inférieur par rapport au modèle global/centralisé et qu'il évite la perte de paquets. L'inconvénient de cette approche est l'entretien et la création des protections multiples de LSP ce qui conduit à une mauvaise utilisation des ressources et à une complexité élevée de gestion.

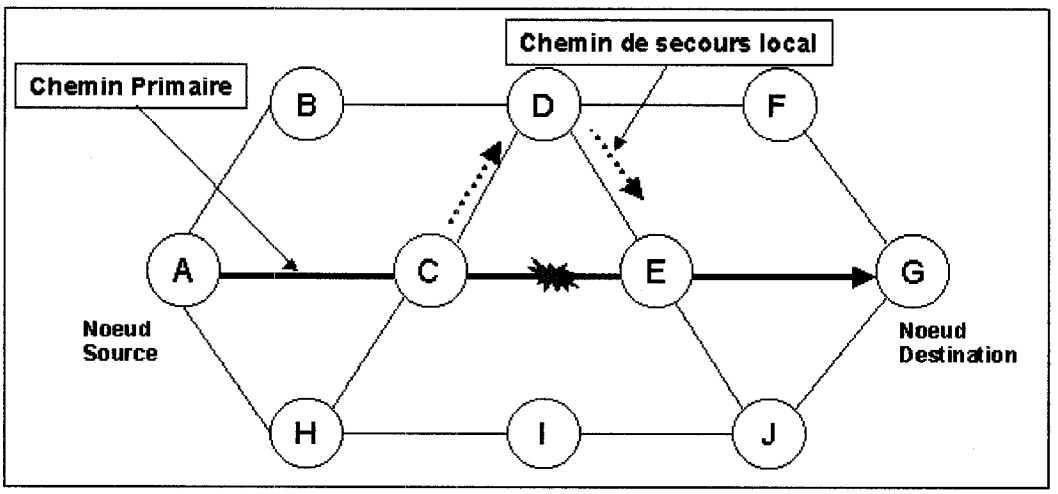

Figure 2.7 Protection Locale

La Figure 2.7 illustre la méthode de protection locale. On a un LSR primaire passant par les nœuds *A*, *C*, *E* et *G*. Le chemin de secours local passe par les nœuds *C*, *D* et *E*. Quand un échec se produit sur le lien (*C*, *E*), le trafic est commuté sur le chemin de secours (*C-D-E*).

Mécanismes de résilience pour les pannes multiples

Dans cette section, nous présenterons deux approches pour résoudre le problème des pannes multiples. La première approche est basée sur une notion de priorité tandis que la seconde approche établit plusieurs niveaux de protection.

a- Approche basée sur la priorité

On considère le scénario présenté à la Figure 2.8, où deux pannes ont lieu au même moment.

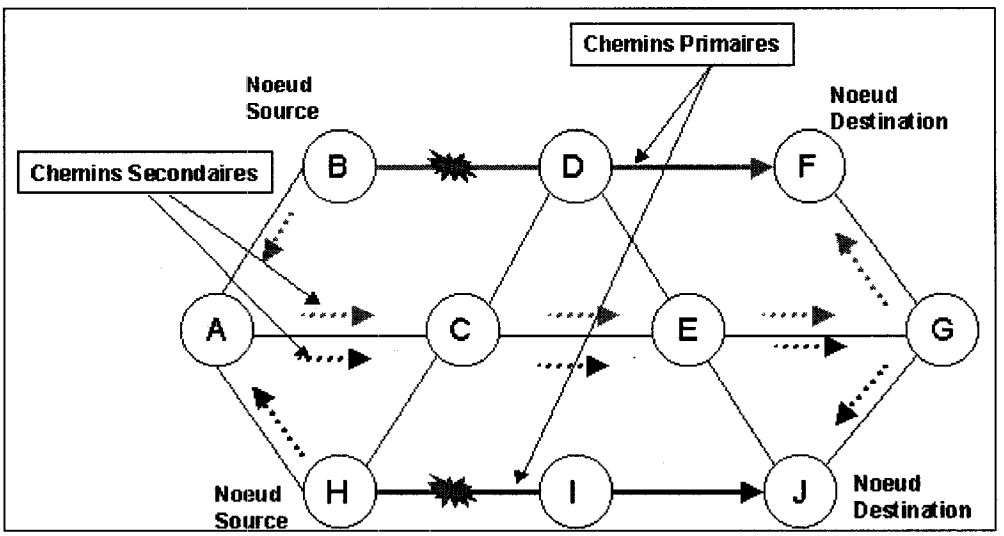

Figure 2.8 Protection basée sur la priorité

On a deux LSP primaires, le premier passe par les nœuds *B*, *D* et *F* ayant comme LSP de secours celui passant par les nœuds *B, A, C, E, G* et *F*. Le deuxieme LSP primaire passe par les nœuds *H*, *I* et *J*. Il a un LSP de secours qui passe par les nœuds *H, A, C, E, G* et *J*. La première panne a lieu sur le lien (*B, D*) tandis que la seconde a lieu sur le lien (*H, I*). Dans cet exemple les nœuds *H* et *B* détectent les panes relatives à leur LSPs en même moment. Si aucune notion de priorité n'est utilisée cette situation peut conduire à une contention sur les ressources partagées. Admettant dans cet exemple que le LSP ayant comme nœud source *H* est plus prioritaire, dans ce cas le chemin de

secours associé à ce LSP sera établi et non pas celui associé avec le LSP primaire de moindre priorité.

b- Protection multi-niveaux

Dans (Marzo et Calle, 2003) plus d'un mécanisme de protection sont utilisés afin d'assurer différents niveaux de protection dépendamment de la classe de trafic. Un scénario multi-niveaux est dynamiquement réalisé en prenant en considération les contraintes de QdS. Cette approche convient aux réseaux ayant une haute exigence en matière de résilience. Néanmoins, cette méthode présente l'inconvénient d'être exigeante en terme de temps et de ressources.

La Figure 2.9 illustre cette approche. On a un LSP Primaire passant par les nœuds *A*, *C*, *E* et *G*. Si le lien (*C*, *E*) tombe en panne, une protection globale est utilisée en utilisant le LSP passant par les nœuds *A*, *B*, *D*, *F* et *G*. Puis, si le lien (*A*, *B*) tombe en panne, la technique de protection locale est utilisée en empruntant le LSP qui passe par les nœuds *A*, *C*, *D*, *F* et *G*.

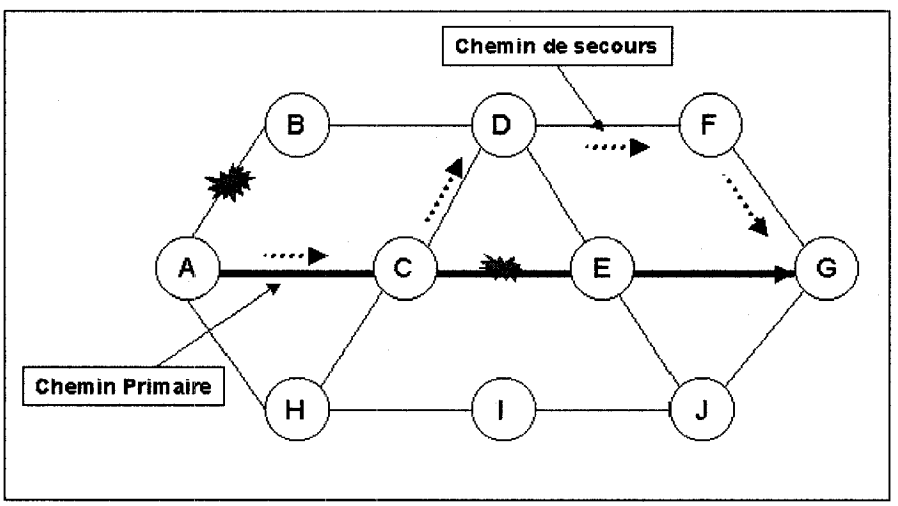

Figure 2.9 Protection multi-niveaux

2.5 Les techniques de notification des pannes

Le groupe de travail IETF-CCAMP a consacré un grand nombre d'efforts pour formaliser et réduire au minimum le temps de rétablissement. Un des aspects les plus intéressants afin de minimiser le temps de rétablissement est l'optimisation de l'étape de notification des pannes. Dans cette section, nous examinons quelques techniques et modèles de notification de pannes. Une comparaison entre ces différentes techniques est également présentée. Deux options sont actuellement exploitées quant à l'attitude à prendre suite à une panne de lien: on procède à une *notification par LSP* ou on fait une *notification par panne.* Dans la première approche, pour chaque LSP passant par le lien ayant eu une panne, on envoie une notification au nœud en charge du déclenchement du mécanisme de restauration pour ce LSP donné. Dans le cas de la notification par panne, on notifie la panne aux nœuds sans envoyer une notification pour chaque LSP passant par le lien endommagé. La principale différence entre la notification par panne et celle par LSP, est le nombre de messages de notification qui sont envoyés. Dans un contexte de réseaux optiques, la notification par LSP peut engendrer une forte charge de signalisation et ainsi exiger plus de ressources réseau que la notification par panne. Quant à la façon de faire la notification, on distingue deux manières : *la notification basée sur la signalisation* et *la notification par inondation.*

2.5.1 Notification basée sur la signalisation

Dans cette approche, le nœud qui détecte la panne, suit le processus suivant :

1- Détecter et énumérer les LSPs affectés par la panne ;

~~3~~2- Pour chaque LSP identifié, envoyer une notification au nœud source correspondant. Cette notification est véhiculée par les nœuds intermédiaires aux différents nœuds source.

De leur côté, chaque nœud source procède aux étapes suivantes dès la réception de la notification de panne :

1- Envoi d'un accusé de réception au nœud ayant détecté la panne;

2- Envoi d'un message de bout en bout de demande de basculement au nœud destination en empruntant le LSP de secours;

3- À la réception de l'accusé de réception du nœud destination, le nœud source commence à envoyer les données sur le LSP de secours.

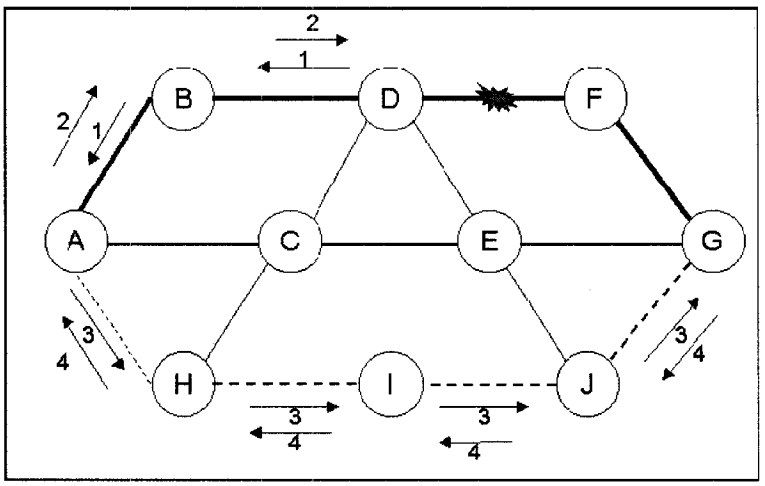

Figure 2.10 Signalisation d'une panne

Ce processus est montré à la Figure 2.10. Dans ce cas-ci, une panne se produit sur le lien (*D, F*). Après que la panne ait été détectée, le nœud *B*, envoie un message d'indication d'échec au nœud source *A*. Les nœuds intermédiaires reçoivent ce message et l'envoient aux nœuds adjacents. Une fois que le message de notification arrive au nœud source, ce dernier envoie un message d'accusé de réception de la notification au nœud *D* (message 2). Ensuite le nœud Source envoie un message au nœud *G* lui indiquant qu'une panne est survenue sur le LSP principal et qu'il faut basculer sur le LSP de secours (message 3). Apres réception de la réponse du nœud *G* (message 4) le transfert commence sur le LSP de secours

Le problème principal de cette approche est le retard occasionné par la mise en file d'attente des messages de notification par les nœuds intermédiaires ainsi que le nombre de messages de notification qui est proportionnel au nombre de LSPs véhiculés par le lien en panne. Ce dernier inconvénient devient très embarrassant dans un contexte de réseaux optique à forte densité.

2.5.2 Notification basée sur l'inondation

Une approche alternative pour aborder la question de la transmission des notifications de panne est d'employer l'inondation (flooding). Au lieu d'envoyer une notification par LSP et le déclenchement d'un processus de recouvrement par LSP, le nœud qui détecte une panne, en informe tous les nœuds du réseau. Dans l'approche de notification basée sur l'inondation, deux choix d'implémentation se présentent. Une approche, serait d'utiliser l'inondation du protocole de routage interne (IGP flooding) comme OSPF et IS-IS, l'autre possibilité d'implémentation serait d'utiliser le protocole LMP. Cette dernière approche parait plus adéquate du fait que LMP inclut déjà des fonctionnalités de gestion de pannes. Le Tableau 2.3 illustre les caractéristiques de chacune des deux techniques de notification.

Tableau 2.3 Comparaison entre la notification par signalisation et par inondation

Inondation	Signalisation
• La notification atteint tous les nœuds de réseau • Le nombre de messages par nœud est déterministe et ne dépend pas de l'état du réseau • Le temps de notification est toujours minimal étant donné que le chemin d'inondation pour une destination donnée est toujours celui ayant le délai le plus faible	• La notification atteint uniquement les nœuds source des LSPs affectés • Le nombre de messages par nœud dépend de l'état du réseau (proportionnel au nombre des LSPs affectés) • Le temps de notification n'est pas garanti étant donné qu'il dépend du chemin et de la longueur du LSP

CHAPITRE III
ROUTAGE INTÉGRÉ DYNAMIQUE ET HYBRIDE AVEC SUPPORT DE LA QUALITÉ DE SERVICE

Dans le chapitre précédent, nous avons présenté une synthèse des mécanismes de survivabilité dans les protocoles MPLS et GMPLS. Nous avons ensuite présenté les protocoles MPLS et GMPLS, la classification des mécanismes de survivabilité et nous avons fait un survol des travaux de recherche et propositions présents dans la littérature. Le protocole MPLS et son extension GMPLS paraissent une approche très prometteuse pour la migration des réseaux actuels vers des réseaux à haut débit avec un plan de contrôle unifié, où les informations de topologie, de disponibilité des ressources et des mécanismes de protection sont connus et partagés par l'ensemble des couches. Une approche tirant profit de ce modèle de collaboration inter-couches et adoptant une politique de protection adéquate selon la classe de trafic, pourrait améliorer l'utilisation des ressources réseau et assurer une survivabilité proportionnelle à l'importance du trafic transporté. Dans le présent chapitre, nous présenterons les motivations, les fondements et les détails algorithmiques de notre approche de routage DHIRQ (*Dynamic Hybrid Integrated Routing with QoS*).

3.1 Motivations et fondements de l'approche proposée

L'approche adoptée pour approvisionner dynamiquement des LSPs dans les réseaux IP/MPLS suit le modèle de réseau en couches (*overlay model*), dans lequel chaque couche réseau est traitée comme une entité séparée avec son propre plan de contrôle. Dans le modèle en couches, il n'y a aucun mécanisme pour qu'une couche identifie et emploie des ressources disponibles dans d'autres couches. La couche IP doit choisir un chemin basé sur la connectivité offerte par la couche inférieure et la bande passante de protection pour le LSP est assignée séparément, indépendamment des possibilités de la protection de la couche inférieure. Bien que ce modèle soit simple à mettre en œuvre, il pourrait mener à une surréservation des ressources de protection.

Nous examinerons la motivation à assurer la survivabilité à l'aide d'un protocole de routage *dynamique* et *intégré* qui offre une meilleure utilisation des ressources réseau et assure une survivabilité adéquate selon la qualité de service exigée. Par dynamique, on entend que les requêtes d'établissement de LSP arrivent en temps réel selon un mode totalement aléatoire et par intégré, on signifie que le protocole de routage a accès à la topologie et aux ressources des couches constituant le réseau grâce au plan de contrôle unifié de GMPLS. Quoique notre objectif soit de concevoir un protocole de routage avec un nombre arbitraire de couches, nous considérons, dans la suite de ce chapitre, un réseau IP sur WDM. Cette supposition est faite pour simplifier la présentation et l'analyse mais elle demeure très réaliste sachant qu'avec le déploiement des réseaux dorsaux optiques, on s'attend à ce que l'architecture de l'Internet du futur converge vers une architecture IP sur WDM avec un plan de contrôle unifié.

3.1.1 Motivations de l'approche

Les motivations derrière notre approche peuvent être résumées en deux points : *la réduction du temps de restauration* après une panne et *l'optimisation des ressources réseau* destinées à la restauration, en prenant en considération le niveau de résilience exigé par le type de trafic à router. Ci-après, on détaillera chacune de ces motivations

A. Réduire le temps de rétablissement après une panne

La réduction du temps de rétablissement est effectuée à deux niveaux : le choix de la méthode de protection adéquate en fonction de la classe de trafic et la prise en considération de la protection au niveau optique lors du choix des chemins.

- ***Choix de la méthode de protection en fonction de la classe de trafic***

Pour illustrer ce point, on va d'abord étudier les étapes qui se produisent avant et après une panne dans le réseau et voir comment on peut réduire le temps de restauration et de ce fait réduire l'impact de la panne sur le rendement global du réseau. Le cycle

typique de recouvrement, peut être résumé par les étapes suivantes (Calle et Marzo, 2004) :

a. Choix des chemins primaires et de protection (algorithme de routage);
b. Établissement des chemins par un mécanisme de signalisation (LDP/RSVP ou CR-LDP/RSVP-TE);
c. Détection de la panne (LMP);
d. Mise en attente avant le déclenchement des processus de recouvrement (Hold off Time);
e. Notification de la panne (LMP);
f. Basculement du trafic sur le chemin de secours;
g. Détection de la réparation du chemin initial (facultatif);
h. Basculement du trafic sur le chemin primaire, une fois qu'on découvre que le défaut a été corrigé ou réparé.

C'est le cycle général des événements qui décrit l'établissement et l'utilisation d'une méthode de protection. Cependant, quelques méthodes de recouvrement n'ont pas besoin de toutes ces étapes. Aussi l'ordre dans lequel se déroulent ces étapes peut différer d'une méthode à une autre. Dans notre cas ce qui importe est le temps de recouvrement noté T_r ci-dessous.

$$\mathbf{T_r = T_d + T_h + T_n + T_b + T_s} \qquad (3.1)$$

Où

$\mathbf{T_d}$: désigne le temps nécessaire à la détection de la panne;

$\mathbf{T_h}$: correspond au temps d'attente entre la détection de la panne et la prise en charge du recouvrement par les couches de haut niveau (IP/MPLS), afin d'accorder le temps aux couches inférieures pour réparer la panne;

$\mathbf{T_n}$: désigne le temps de notification;

$\mathbf{T_s}$: est le temps nécessaire pour trouver un chemin de secours ;

$\mathbf{T_b}$: le temps de basculement du LSP primaire au LSP de secours.

Dans la relation (3.1), les facteurs que nous essayons d'optimiser sont le temps de notification T_n, le temps de recherche du chemin de secours T_s et le temps d'attente T_h. Les autres facteurs sont liés à la technologie de la couche inférieure et, de ce fait ne peuvent être optimisés. Ci-après, on exposera les moyens pour optimiser le temps de notification, le temps de recherche du chemin de secours et le temps d'attente dépendamment de la classe de trafic.

- ***Temps de notification***

Le temps de notification est le délai entre la détection de la panne par le nœud le plus proche et le moment où la procédure de recouvrement est initiée. La notification se fait par l'envoi d'un message de signalisation par le nœud qui détecte la panne au nœud en charge de l'initiation de la restauration. Le temps de notification est variable selon la méthode de protection adoptée et est étroitement lié à la « distance » parcourue par le signal de notification. Dans le cas d'une protection locale, le nœud qui détecte la panne initie lui-même la restauration. De ce fait, le délai de notification est nul. Dans le cas de la protection globale, ce temps dépend du nombre de nœuds (sauts) entre le lien en panne et le nœud source. Ainsi, avec un délai de notification nul, la protection locale est à préconiser dans le cas de classe de trafic de type mission critique et temps réel, les protections globale et segment sont utilisées pour protéger des trafics moins exigeants.

- ***Temps de recherche du chemin de secours***

C'est le temps que cela prend pour trouver un chemin de secours disjoint du chemin primaire. Dans le cas des classes de trafic temps réel et mission critique, on préconise le calcul du chemin de secours au même moment que le calcul du chemin primaire, ce qui signifie que le temps de recherche du chemin de secours après la panne est nul. Dans le cas des classes peu exigeantes en terme de QdS, on détermine le chemin de secours après la panne.

- ***Temps d'attente***

C'est le temps d'attente entre la détection de la panne et la prise en charge du recouvrement par les couches de haut niveau (IP/MPLS), afin d'accorder le temps aux couches inférieures de réparer la panne. Généralement, ce délai d'attente est mis à 50 ms

sans aucune garantie que la couche inférieure assure une protection du lien. On propose que ce délai d'attente soit initialisé en fonction du niveau de protection offert à la couche optique. Ainsi, en absence de protection, ce délai doit être nul afin de permettre le déclenchement de la protection IP/MPLS dès la réception de la notification de la panne. D'où un gain considérable en terme de délais de recouvrement.

- ***Prise en considération de la protection au niveau optique lors du choix des chemins***

Il est bien évident que la protection au niveau des couches inférieures offrent de meilleurs temps de complétion que ceux de la couche IP. En effet, une protection de type SONET peut rétablir la communication dans un délai compris entre 50 ms et 60 ms après une panne. De ce fait, on propose, grâce au plan de contrôle unifié de GMPLS, de prendre en considération la protection optique lors du choix du LSP primaire en favorisant les liens protégés à la couche optique.

B. Optimiser l'utilisation des ressources réseau destinées à la restauration

L'optimisation des ressources de restauration est obtenue en adoptant d'une part une stratégie de partage des liens de secours qui protégent plus d'un seul LSP primaire, et d'autre part en favorisant le passage par les liens protégés à la couche optique. Ainsi, il n'est pas nécessaire de les protéger à la couche IP. Tous les LSPs qui partagent les mêmes ressources de restauration doivent être disjoints pour éviter que plus d'un LSP soit affecté par une seule panne. Aussi, la largeur de bande de restauration peut être employée pour transporter les trafics préemptibles qui peuvent être interrompus si la largeur de bande est nécessaire pour la restauration. D'où une utilisation efficace des ressources réseau.

3.1.2 Fondements de l'approche

Nous identifions les fondements du routage dynamique intégré proposé et présentons les raisons pouvant justifier nos choix :

- ***Algorithme intégré*** : en profitant du plan de contrôle unifié de GMPLS, l'algorithme proposé a la connaissance combinée des ressources et de la topologie à la couche IP et à la couche optique. Une telle connaissance permettra, à notre avis, de mieux utiliser la capacité de réseau en éliminant l'attribution superflue de largeur de bande. En outre, la connaissance combinée de la topologie physique et logique permet le choix efficace des chemins en favorisant les liens ayant une protection au niveau chemin optique.

- ***Protection hybride contre l'échec*** : la protection proposée des LSPs est une protection hybride locale/globale, selon la classe du trafic. Ayant pour objectif de réduire le temps de recouvrement et la consommation des ressources réseau, une méthode de protection est proposée pour chacune des quatre classes de résilience définies par Autenrieth et Kirstädter (2002). On préconise une protection locale en favorisant les liens à protection optique pour la classe de trafic temps réel et mission critique. Les protections globale et segment sont utilisées pour les classes moins exigeantes.

- ***Approvisionnement dynamique*** : l'approche proposée permet le routage dynamique des requêtes LSP dans un réseau IP sur WDM. On préconise une approche dynamique pour la raison suivante : l'approvisionnement de chemin optique (Lightpath) dans les réseaux optiques assume généralement une matrice de trafic statique permettant la planification et l'optimisation globale hors ligne (off line). Cette approche est raisonnable sachant qu'en pratique les chemins optiques sont quasi statiques. Cependant, ce n'est pas le cas pour les réseaux de paquet (IP), où les demandes de connexions et de rupture de connexions sont faites sur demande, sans aucune connaissance préalable du trafic. Ceci rend nécessaire un algorithme de type dynamique. Néanmoins, ceci ne veut pas dire qu'une approche totalement et uniquement dynamique est toujours la meilleure, car cela peut mener à une haute probabilité de blocage du faite que le réseau

n'est pas optimisé d'une façon globale. Ainsi, notre approche doit faire partie d'un système global d'approvisionnement et d'ingénierie de trafic. Un système hybride en ligne/hors ligne (on-line/off line) peut être consideré. Comme illustré à la Figure 3.1, le réseau passe par une étape initiale de dimensionnement faite hors ligne en prenant en considération la prévision du trafic et un modèle d'affectation des probabilités de panne. Cette première phase donne naissance à une topologie qui sera utilisée par notre solution afin de répondre aux demandes dynamiques de LSP. On suggère que le réseau soit périodiquement optimisé de façon globale, en prenant en considération les statistiques relatives aux pannes. Le détail d'un tel système sort du cadre de cette recherche et peut être considéré dans des travaux futurs.

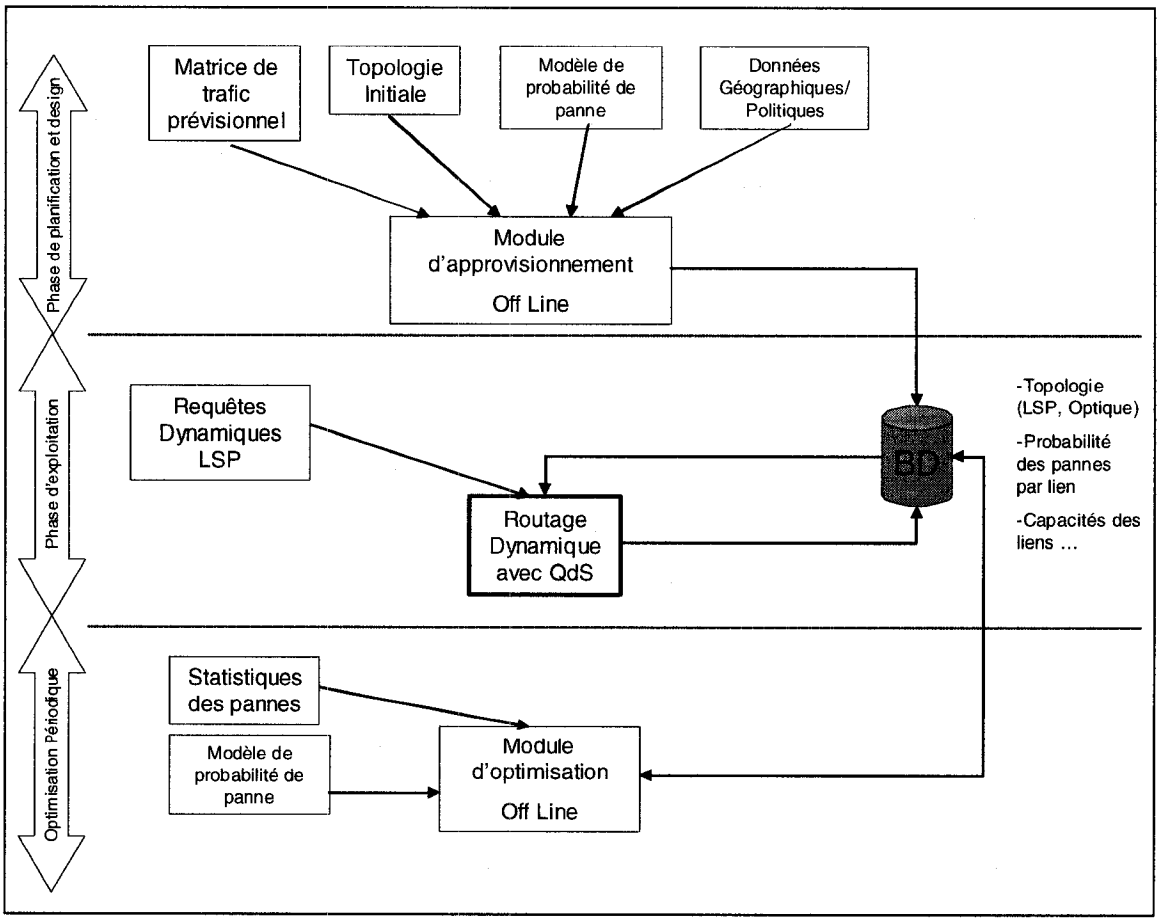

Figure 3.1 Positionnement de l'approche DHIRQ

3.2 Solution proposée

Cette section présente la solution proposée dans l'approche DHIRQ. Nous analyserons les principaux éléments algorithmiques et la modélisation adoptée.

3.2.1 Modélisation du problème

On considère un réseau IP sur WDM avec un plan de contrôle unifié GMPLS. Nous modélisons ce réseau sous la forme d'un graphe G = (*N*, *L*) où *N* est l'ensemble des nœuds et *L* l'ensemble de liens à la couche optiques (lights path). On suppose que le dimensionnement initial est fait de la façon illustrée à la Figure 3.2, en prenant comme paramètres initiaux : une matrice de trafic prévisionnel, un modèle de probabilité de panne et les données géographiques.

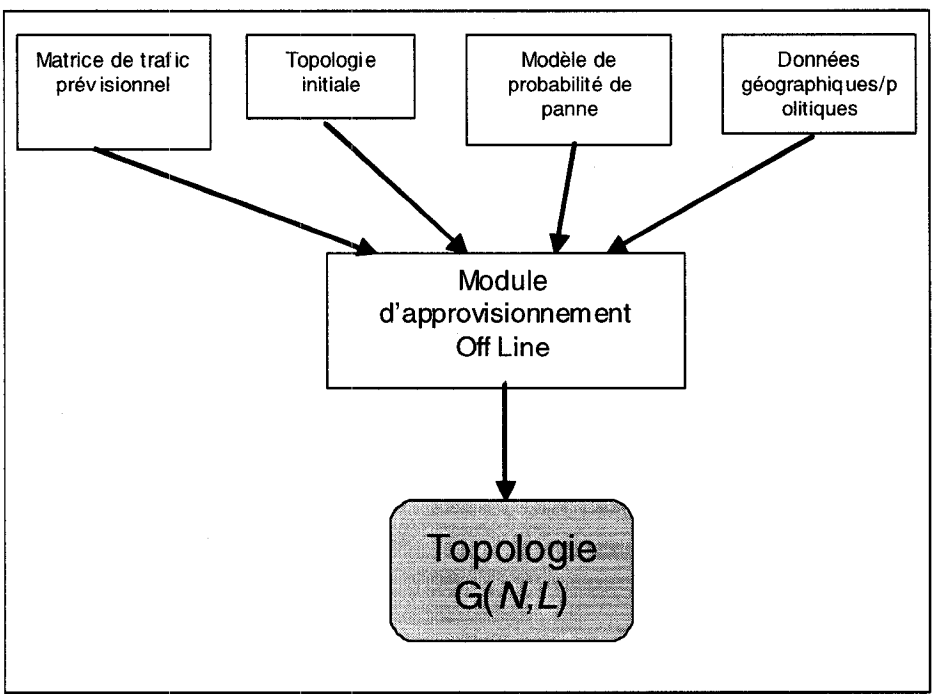

Figure 3.2 Dimensionnement initial du réseau

On suppose que grâce à un mécanisme de signalisation, chaque nœud dispose d'une base de données avec les attributs suivants, associés aux liens auxquels il est connecté :

- ***Les capacités en bande passante :***

  C_g = *Capacité globale du lien*

  C_p = *Capacité réservée pour les liens primaires*

  C_s = *Capacité réservée pour les liens de secours*

  C_{pr} = *Capacité utilisée par un trafic de faible importance, en l'absence de panne*

  C_l = *Capacité libre.*

- ***Probabilité de panne du lien***

- ***Information sur la protection***

  Le type de protection de lien représente les possibilités de protection qui existent pour un lien au niveau de la couche optique. On considère les types suivants :

  - *Non protégé* : Si le lien n'est pas protégé par aucun autre lien au niveau de la couche optique;
  - *Partagé* : Si le lien est protégé par un autre lien et qu'un partage de lien de protection est appliqué;
  - *Dédié 1:1* : le lien est protégé par un lien dédié de type 1:1;
  - *Dédié 1+1* : le lien est protégé par un lien dédié de type 1+1;
  - *Amélioré* : le lien est protégé par un mécanisme plus fiable que 1+1 (i.e. 4 fibres BLSR/MS-SPRING).

L'objectif de notre approche est de trouver un chemin primaire LSP_p, protégé par un LSP_s secondaire, pour toute requête dynamique de LSP en prenant en considération la classe à laquelle appartient le trafic en question. On adopte une classification de trafic selon l'exigence en matière de résilience selon le modèle défini par Autenrieth et

Kirstädter (2002). Quatre classes de résilience distinguées par leur temps de restauration sont définies : *Resilience Class 1 (RC1), Resilience Class 2 (RC2), Resilience Class 3 (RC3), Resilience Class 4 (RC4).*

- RC1 (*Resilience Class 1*) : le trafic possède les plus grandes exigences en terme de résilience avec des temps de restauration inférieurs à 100 msec;
- RC2 (*Resilience Class 2*) : le trafic requiert une qualité de résilience modérée avec des temps de restauration de l'ordre de 100 msec à 1 seconde;
- RC3 (*Resilience Class 3*) : le trafic possède des contraintes de qualité de service faible et exige des temps de restauration de l'ordre de 1 sec à 10 sec;
- RC4 (*Resilience Class 4*) : le trafic n'a aucune contrainte de résilience et peut être préemptible en cas de panne.

3.2.2 Schéma global de la solution et algorithmes

La solution proposée est un algorithme à deux étapes : la première étape consiste à trouver le LSP primaire selon les contraintes spécifiées dans la requête LSP, et la seconde étape permet de trouver un chemin de secours selon un mécanisme de protection approprié à la classe de résilience associée au trafic en question. La Figure 3.3 illustre le schéma global de fonctionnement de notre approche.

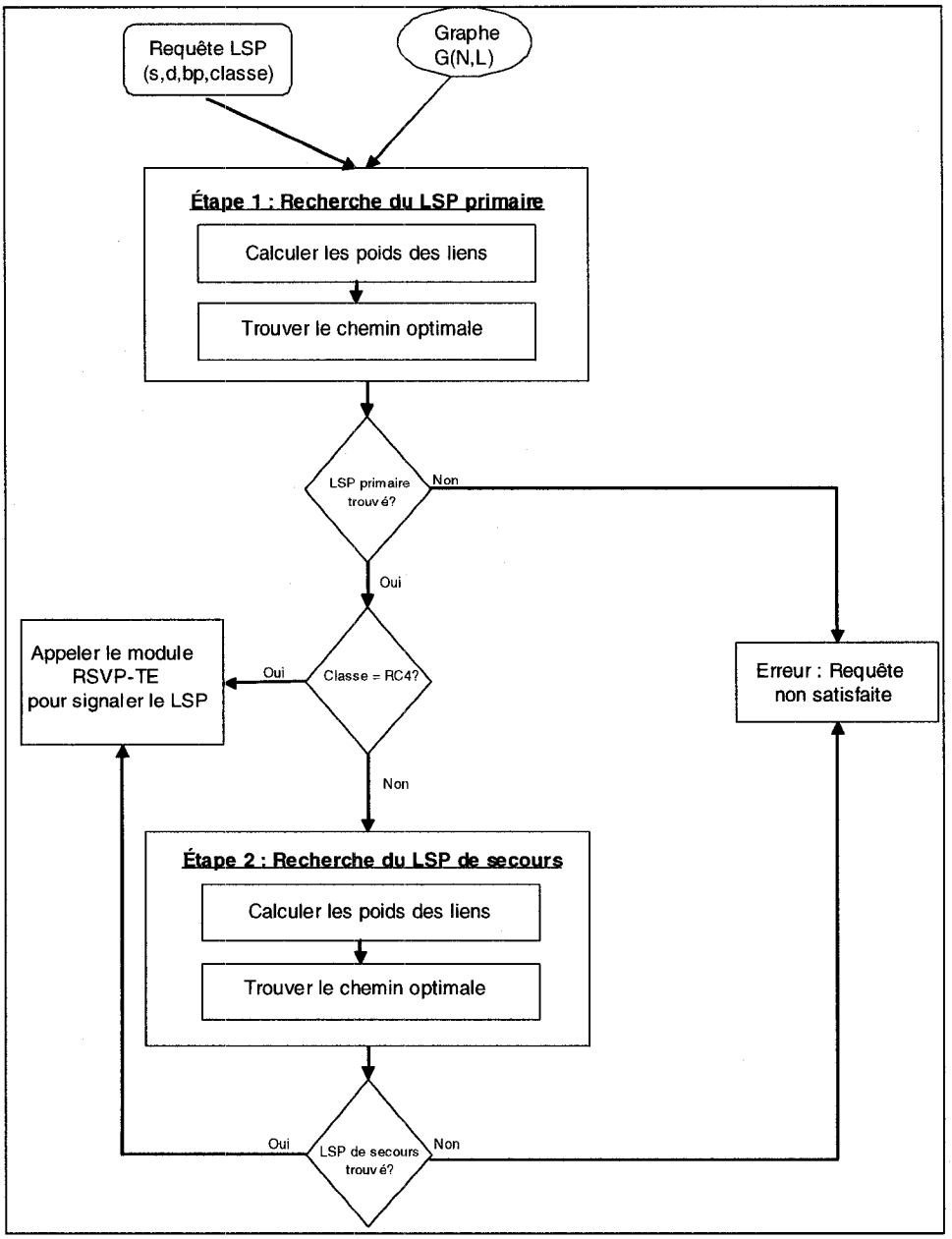

Figure 3.3 Schéma global de la solution

Lors de la première étape, on considère la topologie réseau modélisée par le graphe G (*N*, *L*) et on utilise les attributs des liens pour déterminer le poids associé à chaque lien et utilisé par l'algorithme de recherche du plus court chemin (Algorithme de Dikjstra). Puis, à la seconde étape on élimine les liens utilisés par le lien primaire, afin

de garantir que le LSP de secours soit disjoint du LSP primaire. Ensuite, nous utilisons les attributs de liens pour déterminer le poids des arcs selon la classe de résilience et enfin on cherche le plus court chemin en utilisant l'algorithme de Diksjtra. Les LSPs de secours partageant la même bande passante protégeant des LSPs primaires qui ne sont pas sujets à des pannes simultanées.

L'approche adoptée pour le choix des LSPs primaires et secondaires est liée à la classe de résilience. En effet, selon la classe de trafic, différentes formulations de poids de liens sont faites. Le Tableau 3.1 résume la stratégie préconisée pour chacune des quatre classes de résilience et les Figures 3.5 et 3.6 presentent respectivement la procédure d'établissement du LSP primaire et celle d'etablissement du LSP de secours.

Tableau 3.1 Stratégie préconisée par classe de résilience

	Classe de Résilience			
	RC1	**RC2**	**RC3**	**RC4**
Requis de résilience	Élevé	Moyen	Faible	Aucun
Temps de recouvrement	10 – 100 msec	100 msec – 1sec	1 sec – 10 sec	N.A.
Mécanismes de résilience à la couche IP/MPLS	Protection Locale	Protection Segment/Globale	Protection Segment/Globale	Restauration
Mise en place du chemin de relève à la couche IP/MPLS	Pré établi	Pré établi	Pré-établi	Aucun
Allocation des ressources	Réservé à l'avance	Réservé à l'avance	Réservé à l'avance	Aucun
Favoriser les liens protégés à la couche optique	Oui	Oui, si le type de protection est « dédié 1 :1 » ou « partagé 1 :N »	Oui, si le type de protection est « partagé 1 :N »	Non (favoriser le passage par des liens non protégés à la couche optique)
Qualité de service après le recouvrement	Équivalente	Peut être réduite	Peut être réduite	Best effort

Entrées :

- La requête LSP (s, d, bp, classe). Où : s : source du LSP à établir
  d : destination du LSP à établir
  bp : bande passante requise pour le LSP (>0)
  Classe : la classe de résilience exigée
- Le graphe G(N,L)

Sortie : Chemin du LSP primaire

Algorithme

/* Affectation des poids à tous les liens du graphe */

Si Classe = RC1

$$Poids[i] = \begin{cases} \infty & Si\ C_l[i] < bp \\ \dfrac{Protection[i]}{C_l[i]} & Si\ C_l[i] \geq bp \end{cases}$$

Si Classe = RC2

$$Poids[i] = \begin{cases} \infty & Si\ C_l[i] < bp \\ \dfrac{Partagé}{C_l[i]} & Si\ C_l[i] \geq bp\ ET\ Protection[i] \leq Dédié1 + 1 \\ \dfrac{Protection[i]}{C_l[i]} & Si\ C_l[i] \geq bp\ ET\ Protection[i] > Dédié1 + 1 \end{cases}$$

Si Classe = RC3

$$Poids[i] = \begin{cases} \infty & Si\ C_l[i] < bp \\ \dfrac{Partagé}{C_l[i]} & Si\ C_l[i] \geq bp\ ET\ Protection[i] \leq Dédié1 : 1 \\ \dfrac{Protection[i]}{C_l[i]} & Si\ C_l[i] \geq bp\ ET\ Protection[i] > Dédié1 : 1 \end{cases}$$

Si Classe = RC4

$$Poids[i] = \begin{cases} \infty & Si\ C_l[i] + (C_s[i] - C_{pr}[i]) < bp \\ \dfrac{C_l[i] + (C_s[i] - C_{pr}[i])}{Protection[i]} & Sinon \end{cases}$$

Appliquer l'algorithme de Dijkstra pour trouver le plus court chemin entre *s* et *d*.

Retourner le chemin (LSP) trouvé

Fin

Figure 3.4 Procédure d'établissement du LSP primaire

Entrées :

LSP à protéger,
Classe de résilience
Graphe (N,L)

Sorties :

LSP de protection

Algorithme

Si classe = RC1

On parcourt le LSP primaire et, pour chaque lien ou groupe de liens consécutifs ayant une probabilité supérieure à un seuil pré-determiné, on trouve un chemin de secours ayant comme source le nœud de départ le premier nœud connecté à un lien ayant la probabilité de panne supérieure au seuil et comme nœud destination le dernier nœud figurant sur la suite des liens a haute probabilité de panne. Lors de la recherche du chemin de secours on considère uniquement les liens ayant $C_s + C_l >= bp$. Ceci nous permet d'optimiser la réservation des ressources de secours :

$$Poids[i] = \begin{cases} \infty & Si\ i \in LSPPrimaire\ OU\ C_s[i] + C_l[i] < bp \\ \dfrac{1}{\max(C_s[i], bp) \times Protection[i]} & Sinon \end{cases}$$

Si classe = RC2 ou RC3

On favorise la protection globale/segment. On démarre le lien de secours à partir du premier nœud dont le lien en aval a une probabilité de panne supérieure à un seuil pré-defini et le nœud destination est le nœud egress. Dans notre recherche du chemin de secours, on favorise les liens qui disposent de $C_s + C_l \geq \alpha.bp$. Le facteur α est compris dans l'intervalle [0,1] et spécifie si la totalité de la bande passante doit être protégée ou juste une partie. La valeur de ce facteur est prédéterminée selon la classe de trafic.

$$Poids[i] = \begin{cases} \infty & Si\ i \in LSPPrimaire\ OU\ C_s[i] + C_l[i] < \alpha.bp \\ \dfrac{1}{\max(C_s[i], \alpha.bp) \times Protection[i]} & Sinon \end{cases}$$

Si classe = 4

Pas de protection.

Retourner le LSP de secours trouvé.

Fin

Figure 3.5 Procédure de sélection du chemin de secours

3.2.3 Scénario d'illustration

Comme mentionné ci-haut, la méthode proposée est composée de deux étapes : la recherche du LSP primaire et la recherche du LSP de secours. Ci-après, on détaillera chacune de ces étapes en donnant un exemple pour chacune des quatre classes de résilience adoptées dans notre proposition.

A. Choix du LSP Primaire

Cas 1 : Choix de LSP pour la classe RC1

Dans le cas de la classe de résilience RC1, on préconise le passage par les liens protégés à la couche optique et dont la capacité libre est élevée. Les poids de chacun des liens du réseau sont assignés selon la relation (3.2), où *poids[i]* désigne le poids du lien *i*, *Protection[i]* désigne le type de protection au niveau optique du lien *i*, $C_l[i]$ est la capacité libre sur le lien *i* et *bp* est la bande passante exigée par le LSP primaire.

$$Poids[i] = \begin{cases} \infty & Si\ C_l[i] < bp \\ \dfrac{Protection[i]}{C_l[i]} & Si\ C_l[i] \geq bp \end{cases} \quad (3.2)$$

Si la capacité libre sur le lien est inférieure à la bande passante exigée par le LSP, le poids de ce lien est mis à l'infini, pour ainsi éviter le passage par ce lien congestionné. Dans le cas où la capacité libre est suffisante, le poids du lien est le résultat de la division de son type de protection par sa capacité libre. Ceci résulte en ce que les liens les moins charges (C_l grande) et ayant une bonne protection optique auront un poids faible et ainsi auront plus de chance d'être choisis par l'algorithme du plus court chemin (Dikjstra). On note que, dans notre approche chacun des cinq types de protection correspond à une constante numérique. Les liens non protégés ont la constante la plus grande et les liens protégés ont des valeurs moins grandes selon le type de protection, de sorte à les favoriser et défavoriser les liens non protégés. Les valeurs numériques adoptées dans l'implémentation sur OPNET sont : pour *Non protégé* c'est 10^6, pour

Partagé c'est 10^4, pour *Dédié 1:1* c'est 500, pour *Dédié 1+1* c'est 100 et pour *Amélioré* c'est 10.

La Figure 3.6 illustre le cas de la recherche de chemin pour un LSP primaire de type RC1. Pour des raisons de simplification, on considère que tous les liens disposent de la même capacité libre qui est largement suffisante pour satisfaire la demande du LSP. On remarque que le chemin emprunté est celui ayant des liens protégés (protection améliorée).

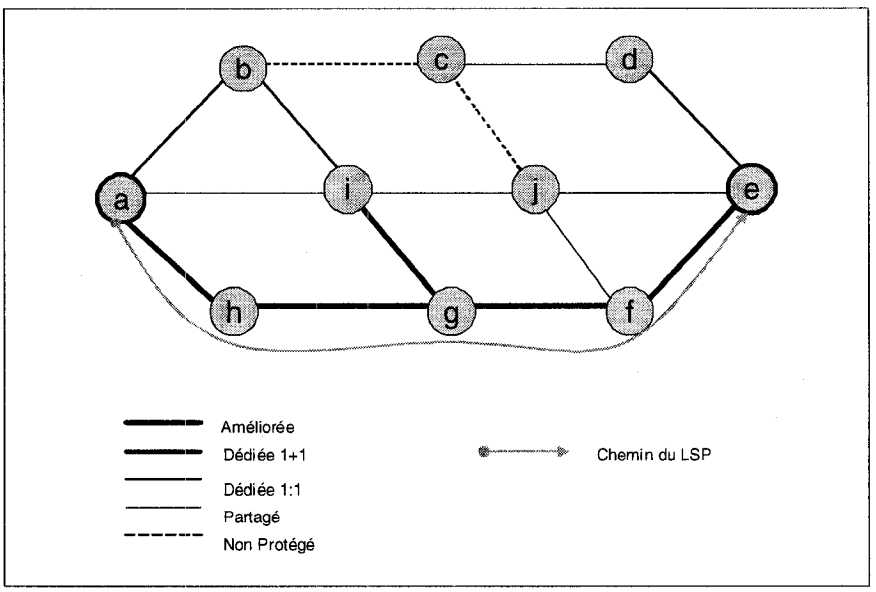

Figure 3.6 Choix de LSP Primaire pour RC1

Cas 2 : Choix de LSP pour la classe RC2

Comme dans le cas de la classe RC1, on affecte des poids à chacun des liens du réseau, en favorisant les liens les moins chargés et les mieux protégés. La principale différence est qu'on va essayer de préserver les liens ayant une protection *Améliorée* et *Dédiée 1+1*, pour la classe RC1. De ce fait, même si on reçoit une demande de RC2 avant les demandes de type RC1, ces liens « précieux » seront toujours disponibles pour être utilises par la classe RC1. Ainsi, dans le calcul du poids, pour tout lien ayant une protection *Améliorée* ou *Dédiée 1+1*, on le rétrograde à un type de protection *Partagée :*

$$Poids[i] = \begin{cases} \infty & Si\ C_l[i] < bp \\ \dfrac{Partagé\ *}{C_l[i]} & Si\ C_l[i] \geq bp\ ET\ Protection[i] \leq Dédié\ 1+1 \\ \dfrac{Protection[i]}{C_l[i]} & Si\ C_l[i] \geq bp\ ET\ Protection[i] > Dédié\ 1+1 \end{cases} \quad (3.3)$$

* : on considère que la protection du lien est de type partagé

La Figure 3.7 illustre le cas de la recherche de chemin pour un LSP primaire de type RC2. Pour des raisons de simplification, on considère que tous les liens disposent de la même capacité libre qui est largement suffisante pour satisfaire la demande du LSP. On remarque que le chemin emprunté est celui ayant des liens protégés avec une protection de type *Dédiée 1:1* et moins.

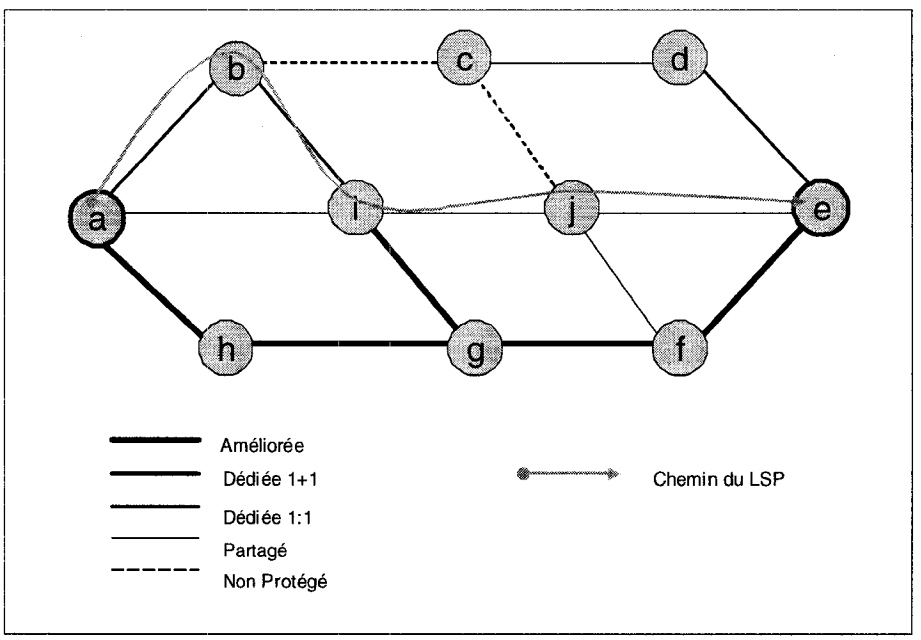

Figure 3.7 Choix de LSP primaire pour RC2

Cas 3 : Choix de LSP pour la classe RC3

Dans le cas de la classe de résilience RC3, on affecte des poids à chacun des liens du réseau, en favorisant les liens les moins chargés et les mieux protégés tout en évitant de passer par des liens ayant une protection réservée aux classe RC1 et RC2. Ainsi, dans le calcul du poids, pour tout lien ayant une protection *Améliorée*, *Dédiée1+1* ou *Dédiée 1:1*, on le rétrograde à un type de protection *partagé :*

$$Poids[i] = \begin{cases} \infty & Si\ C_l[i] < bp \\ \dfrac{Partagé^*}{C_l[i]} & Si\ C_l[i] \geq bp\ ET\ Protection[i] \leq Dédié\ 1:1 \\ \dfrac{Protection[i]}{C_l[i]} & Si\ C_l[i] \geq bp\ ET\ Protection[i] > Dédié\ 1:1 \end{cases} \quad (3.4)$$

* : on considère que la protection du lien est de type partagé

La Figure 3.8 illustre le cas de la recherche de chemin pour un LSP primaire de type RC3. Pour des raisons de simplification, on considère que tous les liens disposent de la même capacité libre qui est largement suffisante pour satisfaire la demande du LSP. On remarque que le chemin emprunté est celui ayant des liens protégés avec une protection de type *Partagé* et moins.

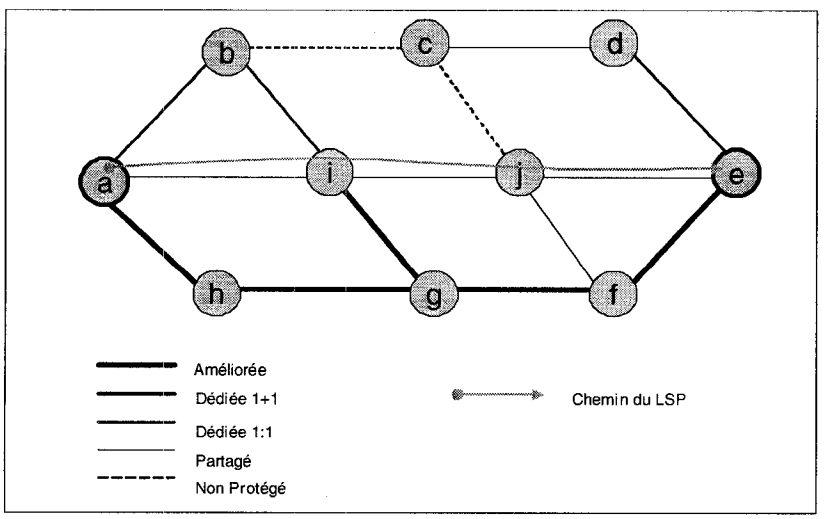

Figure 3.8 Choix de LSP Primaire pour RC3

Cas 4 : Choix de LSP pour la classe RC4

Pour la classe de résilience RC4, on préconise le passage par des liens non protégés et/ou ayant une capacité reservée pour la protection de LSP. Étant donné, la moindre importance du trafic de la classe RC4, ce dernier utilisera les capacités réservées pour la protection pour les LSPs de type RC1, RC2 et RC3. En cas de panne, les LSP de la classe RC4 peuvent être arrêtés pour permettre la restauration des LSPs des classes supérieures. Dans ce cas, le poids est calculé comme suit :

$$Poids[i] = \begin{cases} \infty & Si\ C_l[i] + (C_s[i] - C_{pr}[i]) < bp \\ \dfrac{C_l[i] + (C_s[i] - C_{pr}[i])}{Protection[i]} & Sinon \end{cases} \quad (3.5)$$

La Figure 3.9 illustre le cas de la recherche de chemin pour un LSP primaire de type RC4. On remarque que le chemin emprunté est celui ayant des liens non protégés ou de faible protection.

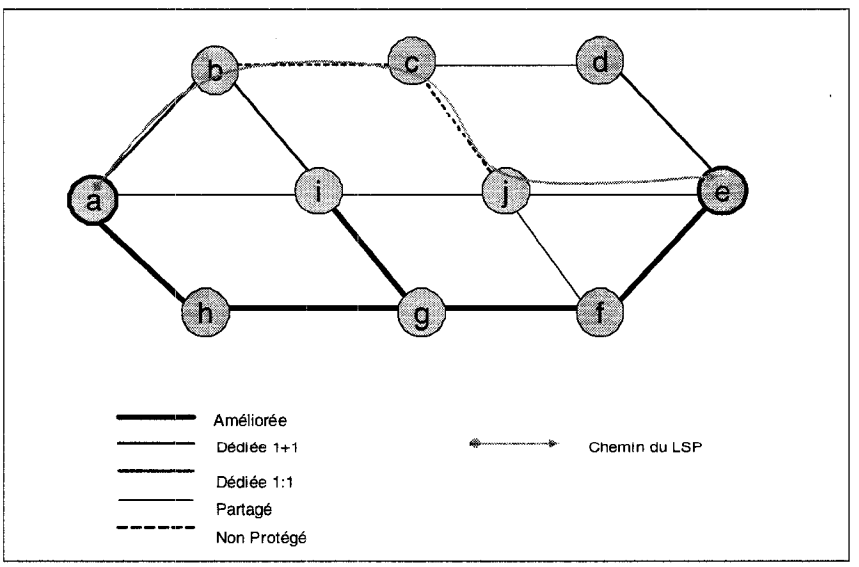

Figure 3.9 Choix de LSP primaire pour RC4

Choix du LSP de secours

Cas 1 : Choix de LSP de secours pour RC1

Pour la classe RC1, on préconise la protection locale. On parcourt les liens du LSP primaire à protéger afin de déterminer quels liens nécessitent une protection selon un seuil de probabilité de panne pré-défini. Pour chaque lien ou groupe de liens consécutifs à protéger, on établit une protection locale. Les poids assignés aux liens lors de la recherche du chemin de secours sont calculés selon la relation (3.6). On favorise les liens qui ne sont pas protégés au niveau optique et qui font déjà partie d'un LSP de secours. Cela nous permet d'une part d'optimiser l'utilisation des ressources réseau et d'autre part de « réserver » les liens protégés au niveau optique, aux LSPs primaires.

$$Poids[i] = \begin{cases} \infty & Si\ i \in LSP\ Primaire\ OU\ C_s[i] + C_l[i] < bp \\ \dfrac{1}{\max(C_s[i], bp) \times Protection[i]} & Sinon \end{cases} \quad (3.6)$$

La Figure 3.10 illustre le cas de la recherche d'un LSP de secours pour un LSP primaire de classe RC1. Le lien (g-f) est protégé par une protection locale (g-i-j-f), étant donné que sa probabilité de panne dépasse le seuil pré-défini pour la classe RC1.

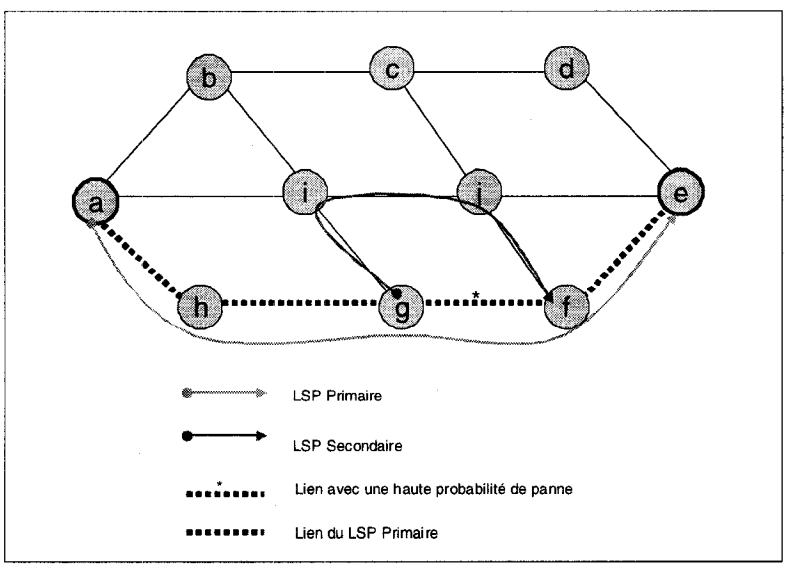

Figure 3.10 Choix de LSP de secours pour RC1

Cas 2 : Choix de LSP de secours pour RC2

Dans le cas de la classe RC2, on préconise une protection globale ou segment. On parcourt les liens du LSP primaire à protéger; dès qu'on trouve un lien ayant une probabilité de panne élevée, on cherche un LSP de secours global ayant comme destination le nœud destination du LSP primaire et comme nœud source le nœud adjacent au lien à protéger. Les poids assignés aux liens lors de la recherche du chemin de secours sont calculés selon la relation (3.7). On favorise les liens qui ne sont pas protégés au niveau optique et qui font déjà partie d'un LSP de secours. Ceci nous permet d'une part d'optimiser l'utilisation des ressources réseau et d'autre part de « réserver » les liens protégés au niveau optique aux LSPs primaires. On admet une dégradation du service, ce qui est exprimé par le facteur α dans la relation (3.7) :

$$Poids[i] = \begin{cases} \infty & Si\ i \in LSPPrimaire\ OU\ C_s[i] + C_l[i] < \alpha.bp \\ \dfrac{1}{\max(C_s[i], \alpha.bp) \times Protection[i]} & Sinon \end{cases} \quad (3.7)$$

La Figure 3.11 illustre le cas de la recherche d'un LSP de secours pour un LSP primaire de classe RC2. Étant donné que la probabilité de panne du lien (*i-j*) est élevée, on démarre un LSP de secours du nœud *i* jusqu'au nœud *e*, passant par les nœuds *g* et *f*.

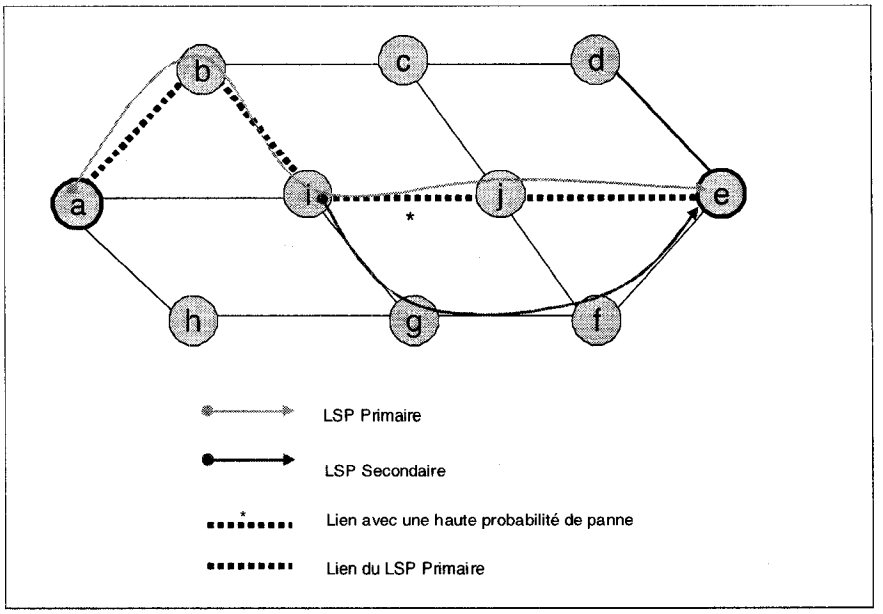

Figure 3.11 Choix de LSP de secours pour RC2

Cas 3 : Choix de LSP de secours pour RC3

La stratégie adoptée pour le choix du LSP de secours dans le cas de la classe RC3 est similaire à celle utilisée pour la classe RC2. La seule différence est dans les seuils de probabilité de panne. En effet, pour la classe RC3, le seuil pour lequel un lien est considéré comme à haut risque de panne est plus élevé que dans le cas de la classe RC2. Ainsi, comme pour la classe RC2, on préconise une protection globale ou segment. On parcourt les liens du LSP primaire à protéger, dès qu'on trouve un lien avec une probabilité de panne supérieure au seuil pré-défini pour la classe RC3, on établit un LSP de secours global. On favorise les liens qui ne sont pas protégés au niveau optique et qui font déjà partie d'un LSP de secours. Les poids des liens sont calculés selon la relation (3.7).

La Figure 3.12 illustre le cas de la recherche d'un LSP de secours pour un LSP primaire de classe RC3. Le lien (i-j) présente une probabilité de panne supérieure au seuil pré-défini pour la classe RC3. On établit un LSP de secours du nœud *i* jusqu'au nœud *e*, passant par les nœuds *b*, *c* et *d*.

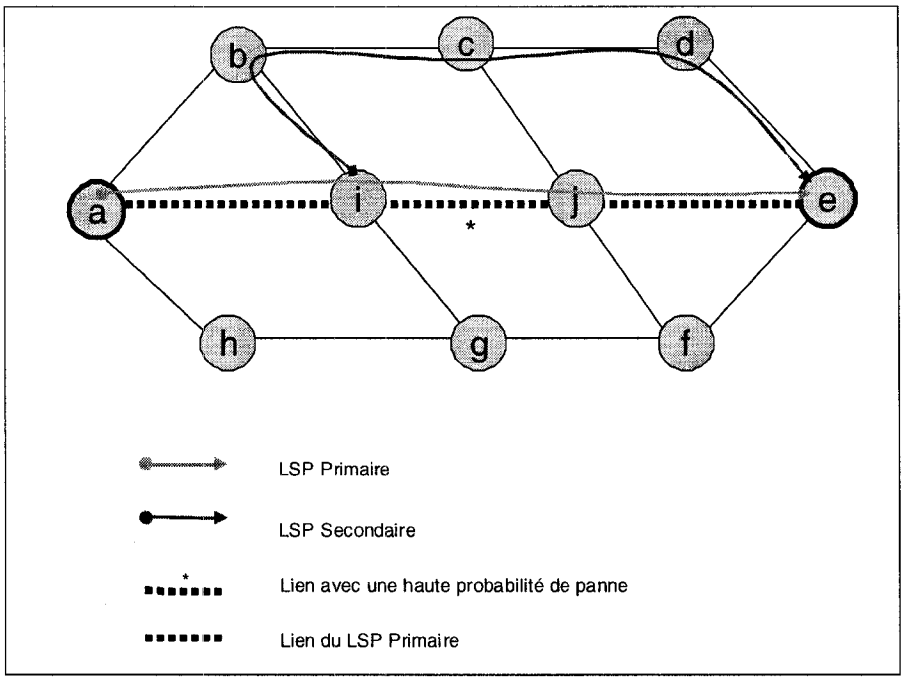

Figure 3.12 Choix de LSP de secours pour RC3

3.3 Complexité de l'algorithme proposé

L'approche proposée se compose de deux étapes principales : une première étape de recherche de chemin primaire et une deuxième étape de recherche du chemin de secours. Dans cette section, on étudiera la complexité algorithmique de chacune de ces deux étapes.

3.3.1 Recherche du chemin primaire

La recherche du chemin primaire est faite en deux phases. Premièrement, on assigne les poids aux liens du graphe représentant le réseau, puis on utilise l'algorithme de Dijkstra pour déterminer le chemin qui optimise les critères exprimés dans la fonction de coût des liens. La Figure 3.13 représente le fonctionnement global de l'étape de recherche du chemin primaire.

Le réseau est représenté par un graphe G (N, L) avec n nœuds et l liens. L'affectation des poids aux liens se fait en O(l). L'initialisation des étiquettes de sommet est en O(n). La recherche du minimum est en O(n) chaque fois, soit O(n^2) en tout. Quant

à l'actualisation, elle nécessite au total l'examen de tous les arcs, soit *l*; l'actualisation d'une valeur est en temps constant d'où O(*l*). Puisque typiquement $n<l<n^2$, la complexité finale est $O(n^2)$. Ceci est vrai si le graphe est représenté par un tableau des successeurs. On peut représenter le graphe par une autre structure (file de priorité) pour laquelle la recherche du minimum est en O(log n). On a ainsi une complexité $O(n \log n + l)$. Cette complexité devient plus intéressante dans le cas où $l<<n^2$. Ainsi, la complexité de l'algorithme proposé est celle de l'algorithme de Dijkstra.

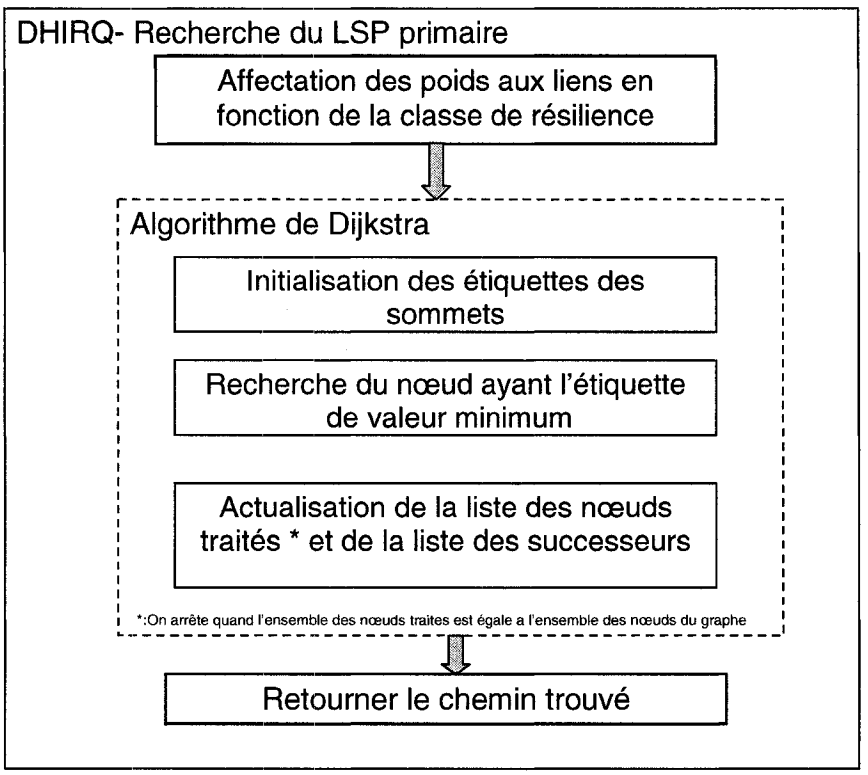

Figure 3.13 DHIRQ-Recherche du LSP primaire

3.3.2 Recherche du LSP Secondaire

La méthode utilisée pour la recherche du chemin de secours dépend de la classe de résilience du trafic transporté. Ainsi, pour la classe RC1, on préconise une protection locale; pour RC2 et RC3, on adopte une protection de type globale ou segment. Ci-après, on étudie la complexité de l'algorithme proposé dans les deux cas de figure : protection

locale et protection globale. Il est à noter que, pour la classe RC4, on ne prévoit aucun mécanisme de protection.

Recherche de chemin secondaire pour les classes de résilience RC2 et RC3 :

La Figure 3.14 illustre les étapes suivies dans ce cas. On commence par parcourir le chemin primaire à protéger et, selon les seuils pré-definis de probabilité de panne, on détermine le nœud source *s* du chemin de secours, puis on affecte les poids aux liens du graphe. On utilise l'algorithme de Dijkstra pour trouver le chemin, de la source s au nœud egress, qui optimise les critères exprimés dans la fonction du poids des liens.

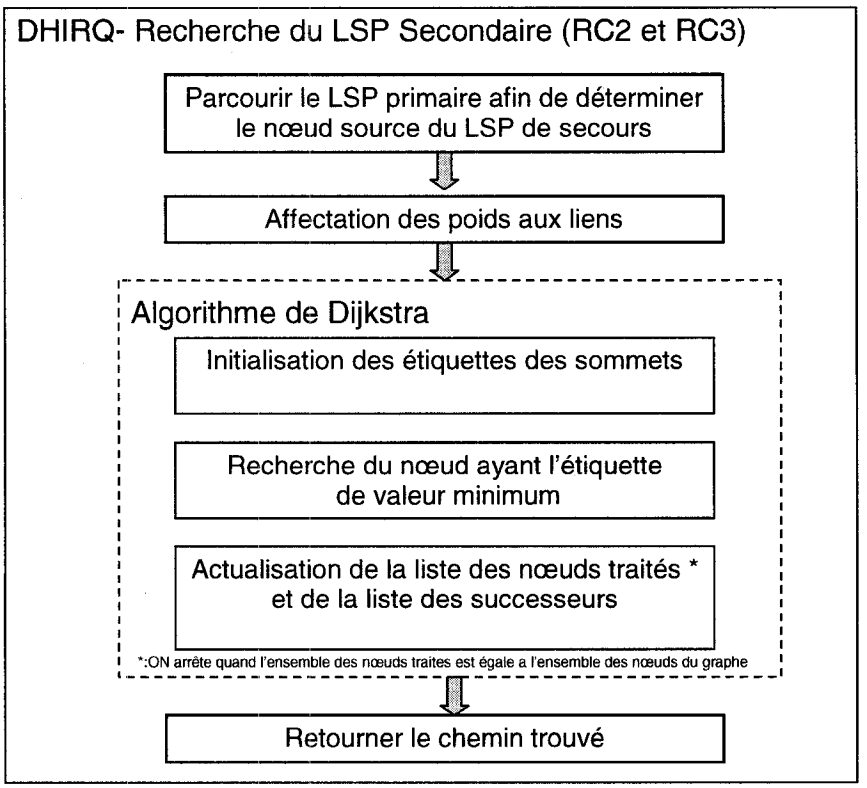

Figure 3.14 DHIRQ Recherche du LSP secondaire RC2 et RC3

Le réseau est représenté par un graphe G (*N*, *L*) avec *n* nœuds et *l* liens. Le parcours du LSP primaire se fait en O(*l*) étant donné que le nombre de liens du LSP

primaire est toujours inférieur ou égal ou nombre d'arcs dans le graphe. L'affectation des poids aux liens se fait en O(l). L'algorithme de Dijkstra a une complexité O(n *log* n +l). Ceci implique que la complexité de l'algorithme proposé de recherche du chemin de secours pour les classes RC2 et RC3 a une complexité de O (n log n + l).

Recherche de Chemin secondaire pour la classe de résilience RC1

Comme dans le cas des deux classes RC2 et RC3, on commence par parcourir le LSP primaire pour déterminer les liens à protéger. La principale différence, c'est qu'au lieu d'établir une protection globale, on adopte un mécanisme de protection locale pour tout lien ou ensemble de liens qui ont une probabilité de panne supérieure au seuil prédéfini. La Figure 3.15 illustre ce cas.

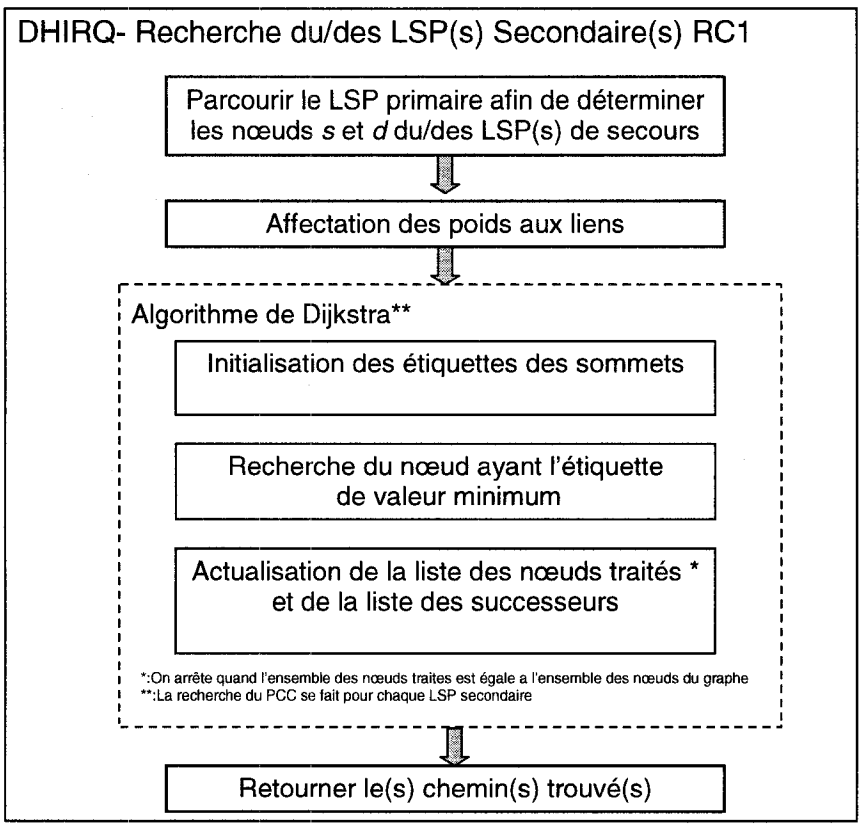

Figure 3. 15 DHIRQ Recherche du/des LSP(s) secondaire(s) RC1

Le réseau est représenté par un graphe G (N, L) avec n nœuds et l liens. Le parcours du LSP primaire se fait en O(l) étant donné que le nombre de liens du LSP primaire est toujours inférieur ou égal au nombre d'arcs dans le graphe. L'affectation des poids aux liens se fait en O (l). L'algorithme de Dijkstra a une complexité O($n \log n + l$); au pire des cas il sera appelé $l/2$ fois. Ceci implique que la complexité de l'algorithme proposé de recherche du chemin de secours pour la classe RC1 est O($n \log n + l$).

CHAPITRE IV
ÉVALUATION DE PERFORMANCE ET RÉSULTATS

Dans le chapitre précédent, nous avons décrit un algorithme de routage dynamique et intégré permettant le choix des LSP primaires et de secours. Cet algorithme tire profit du plan unifié de GMPLS en prenant en considération les ressources réseau en termes de protection optique et de disponibilité de bande passante. De plus, le mécanisme de protection est adaptatif aux exigences de résilience de chacune des classes de trafic transportées. Dans le présent chapitre, nous confronterons expérimentalement notre approche de routage dynamique (DHIRQ) avec l'algorithme CSPF implémenté dans OPNET Modeler. Ces comparaisons expérimentales visent à déterminer les gains et les pertes de notre approche par rapport à l'algorithme CSPF. Nous commençons ce chapitre en détaillant l'implémentation et le prototypage de notre modèle sur l'outil de simulation OPNET. Par la suite, nous élaborons le plan d'expérience, et finalement nous analysons les résultats.

4.1 Implémentation et prototypage du modèle

Dans cette section, nous présenterons les modifications apportées au modèle CSPF disponible sur OPNET Modeler afin de modéliser notre approche de routage DHIRQ. En premier lieu, nous présenterons les modules et fonctions utilisés par CSPF, puis détaillerons les modifications apportées à ces modules et fonctions pour modéliser notre approche.

4.1.1 Implémentation du protocole CSPF dans OPNET Modeler

Le protocole CSPF (Constraint-based Shortest Path First) se base sur OSPF ou IS-IS pour calculer le plus court chemin à travers un réseau. CSPF calcule une route optimale en se basant sur un ensemble spécifique de contraintes comme le nombre de routeurs intermédiaires, le délai de transmission maximal ou la bande passante. La route optimale trouvée par CSPF est utilisée, par la suite, par le module RSVP-TE pour signaler les

LSPs. La Figure 4.1 illustre l'interaction entre les fonctions implémentées dans OPNET lors de la signalisation d'un LSP dynamique.

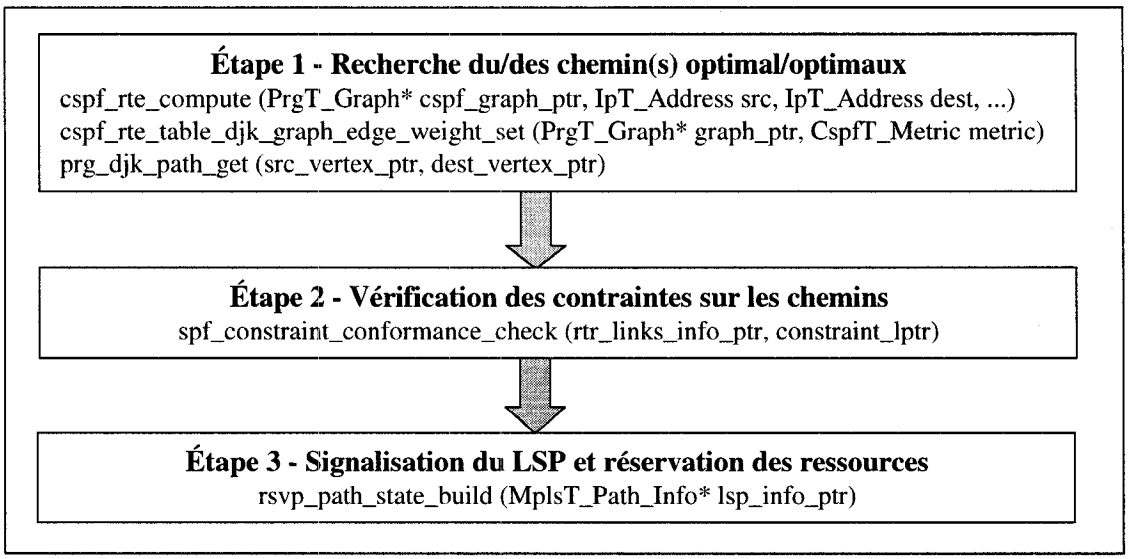

Figure 4.1 Etapes d'établissement d'un LSP dynamique avec CSPF

Lors de l'étape de recherche des chemins optimaux, OPNET fait appel à trois principales fonctions : *cspf_rte_compute*, *cspf_rte_table_djk_graph_edge_weight_set* et *prg_djk_path_get*. La fonction *prg_djk_path_get* implémente l'algorithme de Dikjstra pour la recherche du plus court chemin en fonction des poids des liens assignés via la fonction *cspf_rte_table_djk_graph_edge_weight_set*. Quant à la fonction *cspf_rte_compute,* elle permet d'une part l'initialisation de la structure de graphe représentant le réseau à simuler et d'autre part d'invoquer les deux fonctions *cspf_rte_table_djk_graph_edge_weight_set* et *prg_djk_path_get*. Seuls les chemins respectant les contraintes sont gardés après la deuxième étape. Puis un seul chemin est élu d'une façon aléatoire et transmis au module RSVP-TE qui procède à la signalisation du LSP et à la réservation des ressources.

4.1.2 Implémentation de l'approche DHIRQ sur OPNET

Comme détaillé au Chapitre 3, l'approche DHIRQ se base sur le plan unifié de GMPLS pour tenir compte, lors du calcul du poids pour la recherche du plus court chemin, de la probabilité de panne, de la protection optique et des capacités en bande passante de chacun des liens. Lors de l'implémentation de l'algorithme DHIRQ sur OPNET, l'accès à l'information sur la configuration de la couche optique et aux capacités en bande passante a constitué le plus grand défi étant donné que le plan de contrôle implémenté dans OPNET suit un modèle en couches (*overlay model*). La solution adoptée consiste à simuler le plan unifié de GMPLS en mettant en place une structure de données partagée et accessible à tous les modules d'OPNET. Cette structure de données contient la configuration du réseau à simuler et tous les paramètres nécessaires pour le calcul des poids de chacun des liens avec l'approche DHIRQ. En effet, la structure partagée contient les capacités en bande passante, les protections optiques et les probabilités de panne pour chacun des liens du réseau. L'information sur les capacités est maintenue à jour d'une façon dynamique en temps réel après l'établissement d'un LSP. La Figure 4.2 montre la définition de la structure de données utilisée dans notre implémentation.

```
typedef struct
{
      IpT_Address       RouterID;
      IpT_Address       Interface;
      double      Cg;   //Capacite Generale du lien exprimee en bps
      double      Cp;   //Capacite reservee pour liens primaires
      double      Cs;   //Capacite reservee pour liens de secours
      double      Cpr;  //Capacite reservee pour Trafics de RC4
      double      Cl;   //Capacite libre sur le lien
      double      ProbPanne;  //Probabilite de panne du lien
      int         ProtectionOptique; //type de la protection optique
} NH_Lien;
```

Figure 4.2 Structure de données simulant le plan unifié de GMPLS

En plus de la structure partagée simulant le plan de contrôle unifié de GMPLS, plusieurs fonctions ont été ajoutées aux modules d'OPNET. Ces fonctions permettent le maintien à jour des données de la structure globale, l'interaction avec les modules d'OPNET et l'implémentation de l'algorithme DHIRQ en tant que tel. La Figure 4.3 illustre le fonctionnement global de l'approche DHIRQ telle qu'implémentée dans OPNET. Par souci de simplification, seules les principales fonctions sont illustrées dans cette figure.

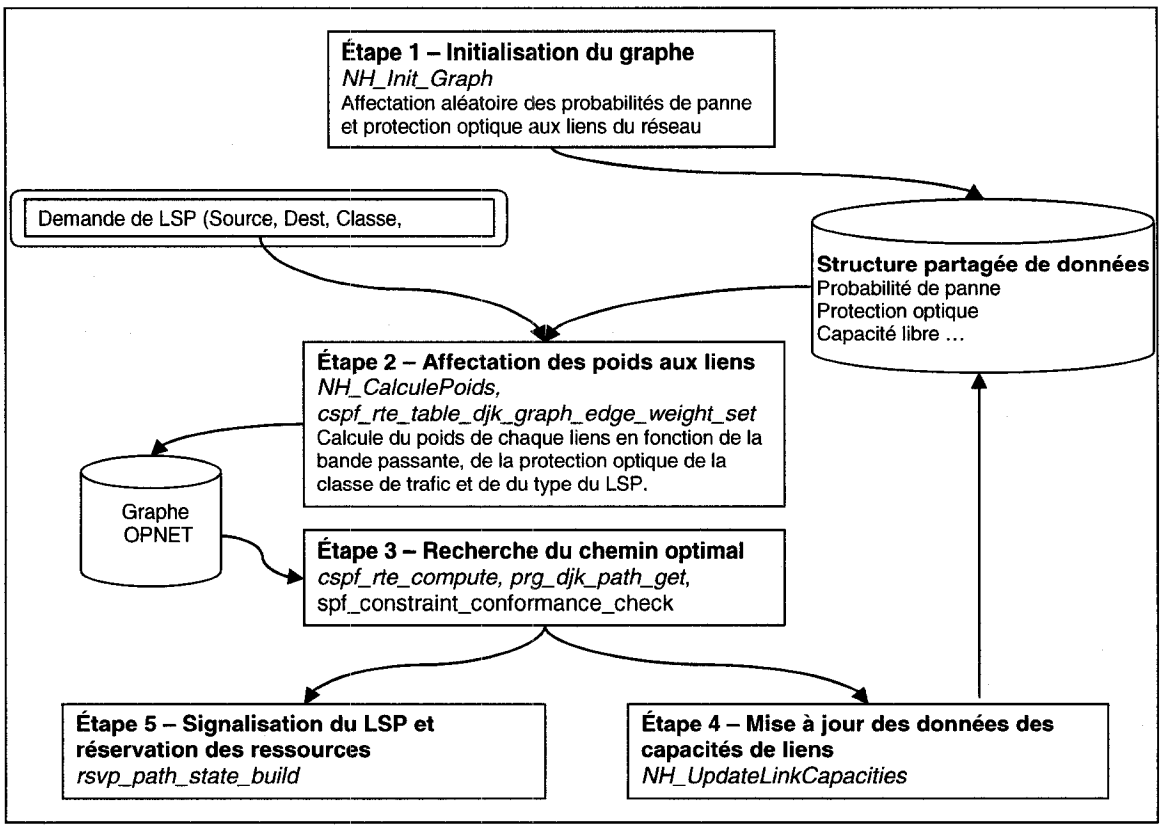

Figure 4.3 Implémentation de DHIRQ dans OPNET

Nous commencons par initialiser la structure globale au début de chaque simulation. Cette phase d'initialisation fait appel à la fonction *NH_Init_Graph* et consiste, principalement, à assigner d'une façon aléatoire les probabilités de panne et protection optique à chacun des liens du réseau. À la réception d'une demande

dynamique d'établissement de LSP, le calcul des poids des liens se fait grâce à la fonction *NH_CaclculePoids* en prenant en considération les données de la structure simulant le plan de contrôle unifié et la nature du LSP en question. Le module de recherche du chemin optimal, étape 3, utilise le graphe OPNET pour trouver le chemin optimisant les contraintes exprimées sur les poids des liens assignés lors de l'étape 2. Une fois le chemin optimal trouvé, on met à jour l'information sur les capacités des liens lors de l'étape 4, en invoquant la fonction *NH_UpdateLinkCapacities*. La signalisation du LSP et la réservation des ressources se fait, comme dans le cas de CSPF, en invoquant le module RSVP-TE d'OPNET.

4.2 Choix des métriques et modélisation des sources de trafic

Dans cette section, nous commencerons par élaborer les métriques utilisées pour l'évaluation de performance. Nous expliquerons ensuite la manière dont nous avons modélisé les sources de trafic.

4.2.1 Choix des métriques

Nous utiliserons deux métriques comme base de comparaison dans notre évaluation de performance : *La probabilité de panne du LSP primaire* et *Le taux d'utilisation des ressources de restauration.*

- *La probabilité de panne du LSP primaire* : mesure la probabilité de panne du LSP choisi. Cette probabilité est calculée en fonction des probabilités de panne de chacun des liens constituant le LSP. Plus la probabilité de panne est moindre, plus le LSP est résiliant aux pannes de liens. En plus, on vérifiera si notre approche respecte la classification de trafic qu'on s'est fixée, à savoir les LSPs de la classe RC1 doivent avoir la plus faible probabilité de panne indépendamment de l'ordre chronologique d'arrivée des requêtes et de la charge des liens.
- *Taux d'utilisation des ressources de restauration* : Un des objectifs de l'approche DHIRQ est d'optimiser les ressources réseau dédiées à la protection. Comme

expliqué au Chapitre 3, cette optimisation est atteinte de deux façons : préconiser le partage des ressources de protection et favoriser les liens protégés au niveau optique lors du choix des LSP primaires. On tentera de vérifier dans notre évaluation de performance quel est le gain en terme d'utilisation de ressource de notre approche.

4.2.2 Modélisation des sources de trafic

Afin de réaliser un prototype réaliste, on a modélisé chacune des quatre classes de trafic par des sources de données ayant les mêmes exigences en termes de résilience et de délais de recouvrement. Ainsi, la classe RC1 est modélisée par du trafic de voix, la classe RC2 par de la vidéo conférence, la classe RC3 par du trafic base de données et la classe RC4 par du trafic http. Dans notre implémentation, nous avons utilisé un total de 20 sources de trafic pour chacune des quatre classes. Les caractéristiques des sources de trafic sont données aux Tableaux 4.1, 4.2, 4.3 et 4.4 pour les classes RC1, RC2, RC3 et RC4 respectivement.

Tableau 4.1 Caractéristiques du trafic de la classe RC1

Paramètres	Valeurs
Encodeur	G.711
Tailles des trames (sec)	4 msec
Taux de codage (*Coding Rate*) (bits/sec)	64 Kbps
Classe de Service DiffServ (*DSCP*)	EF
Trames de voix par paquets	1
Délai de compression	0.02 sec
Délai de décompression	0.02 sec

Tableau 4.2 Caractéristiques du trafic de la classe RC2

Paramètres	Valeurs
Vidéo conférence Haute Résolution	
Inter-arrivée des images	15 images/sec
Taille des images (octets)	128X240 pixels
Classe de Service DiffServ (*DSCP*)	AF31

Tableau 4.3 Caractéristiques du trafic de la classe RC3

Paramètres	Valeurs
Nom	Accès Base de données – charge moyenne
Type des transactions	Requêtes 100%
Taille de la transaction	512 Octets
Inter-arrivée des transactions	Exp(12)
Classe de Service DiffServ (*DSCP*)	AF13

Tableau 4.4 Caractéristiques du trafic de la classe RC4

Paramètres	Valeurs
Nom	Navigation WEB
Spécification http	http 1.1
Inter-arrivée des pages (secondes)	Exp(60)
Type de service	Best Effort

4.3 Plan d'expérience

Dans cette section, nous allons d'abord identifier les facteurs à mesurer lors des simulations. Ensuite, nous décrirons les tests effectués pour la validation du modèle.

4.3.1 Identification des facteurs

Afin d'évaluer la performance et valider notre modèle, nous avons procédé à plusieurs sessions de simulation. À la fin de chaque session, les valeurs des deux métriques de comparaison ont été prises afin de procéder à une comparaison avec le protocole CSPF implémenté dans OPNET. Pour chacune des sessions de simulation, nous avons étudié l'impact de deux facteurs variables : *l'ordre d'arrivée des*

requêtes dynamiques et *le taux d'utilisation des liens.* Ces deux facteurs sont pertinents pour les raisons suivantes :

- *Ordre d'arrivée des requêtes LSP* **:** l'objectif de notre algorithme est de router des demandes LSP de façon dynamique et en temps réel, ce qui signifie que l'ordre des arrivées des requêtes n'est pas connu à l'avance. Ceci pose un défi sachant qu'on veut différencier les classes de trafic dans le réseau et que les liens sont choisis pour favoriser ou défavoriser le trafic selon la classe de résilience à laquelle il appartient. En effet, l'aspect dynamique des requêtes peut faire en sorte que les demandes qui arrivent en premier vont emprunter des liens de « bonne qualité » ayant une large bande passante et une meilleure protection optique. Notre approche essaie d'éviter que l'affectation des liens soit liée à l'ordre chronologique des arrivées mais plutôt à la classe de résilience. Ainsi, une demande de classe RC1, devrait être satisfaite même si plusieurs demandes de classes inférieures sont déjà faites. Dans notre évaluation de performance, on étudiera l'effet de l'ordre d'arrivée des requêtes sur le comportement de notre algorithme. On considérera plusieurs cas où les requêtes des quatre classes de résilience sont faites selon différents ordres.

- *Taux d'utilisation des liens* : Ce facteur influence le calcul des poids des liens lors du choix du LSP primaire et de secours.

Le Tableau 4.5 représente les facteurs variables des simulations et leurs descriptions.

Tableau 4.5 Facteurs et niveaux choisis pour la simulation de DHIRQ

Facteurs		Niveaux	
Nom	**Symbole**	**Nom**	**Description**
Ordre d'arrivée des requêtes LSP	A	RC1-RC2-RC3-RC4	Une requête RC1 arrive en premier suivie de RC2, RC3 et RC4 respectivement
		RC2-RC1-RC3-RC4	Une requête RC2 arrive en premier suivie de RC1, RC3 et RC4 respectivement
		RC3-RC2-RC1-RC4	Une requête RC3 arrive en premier suivie de RC2, RC1 et RC4 respectivement
		RC4-RC3-RC2-RC1	Une requête RC4 arrive en premier suivie de RC3, RC2 et RC1 respectivement
Taux d'utilisation des liens	U	Grand	80 %
		Moyen	60 %
		Faible	25 %

Afin d'observer l'influence des paramètres représentés au Tableau 4.5 sur les métriques de comparaison qu'on s'est fixées, nous avons effectué une série de tests. À chaque test, nous avons considéré un des facteurs constant (i.e. U = 60 %) et on a fait varier l'autre facteur. Ceci donne 12 cas de tests possibles. En plus, à fin d'avoir des valeurs et des tests significatifs, nous avons roulé chacun des 12 tests 100 fois avec une configuration de probabilités et de protections optiques assignée de façon complètement aléatoire au début de chaque test. Ainsi, à la fin de nos sessions de simulations, 1200 tests on été faits pour le protocole CSPF et 1200 autres tests ont été faits pour le

protocole DHIRQ. Aussi, étant donné que dans chaque session de test, 4 demandes de LSPs sont faites (une demande par classe) ceci implique que 4800 demandes de LSPs ont été faites pour chacun des deux protocoles évalués.

4.3.2 Topologie utilisée pour les tests

Le réseau utilisé pour effectuer la simulation est représenté à la Figure 4.4. Les sources de trafic pour chacune des quatre classes de résilience sont définies dans des sous-réseaux afin d'alléger la présentation de la figure. Les liens constituant le réseau dorsal ont une capacité OC3 (148 Mbps). La durée d'une simulation est de 300 secondes. Le premier LSP est établi au temps 150 secondes, le deuxième LSP au temps 180 secondes, le troisième au temps 210 et le quatrième au temps 240 secondes. Tous les LSPs sont de type dynamique, ce qui signifie que seules la source et la destination sont définies avant le début de la simulation. Le chemin emprunté par le LSP est déterminé lors de la simulation en prenant en considération la classe de trafic, la charge des liens ainsi que le niveau de la protection optique.

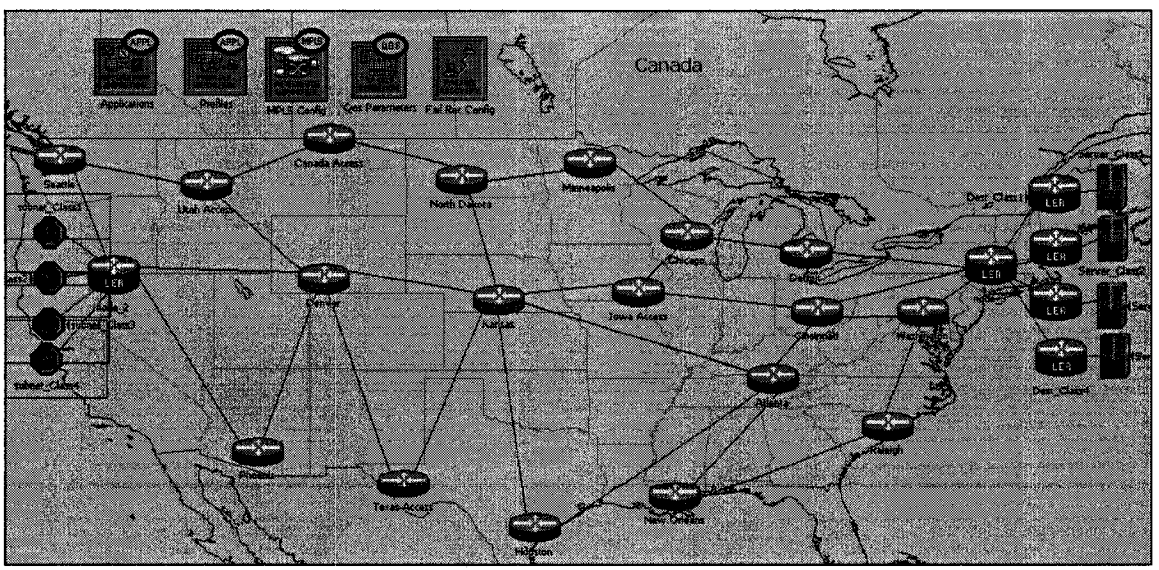

Figure 4.4 Topologie utilisée pour les tests

4.4 Analyse des résultats

Dans cette section, nous analysons les résultats obtenus après la série des tests effectués pour le protocole de routage CSPF et notre approche DHIRQ. Nous détaillons les résultats obtenus pour la première phase de notre algorithme, à savoir le choix du LSP primaire. Puis, nous analysons les résultats des tests pour la seconde phase qui est la protection du LSP primaire.

4.4.1 Analyse des résultats de la première phase (Choix des LSP primaires)

Comme détaillé au Chapitre 3, l'approche DHIRQ est un algorithme à deux étapes : une première étape de choix de LSP primaire suivie de l'étape de protection du chemin primaire. Dans cette section, nous analysons les résultats relatifs au choix du LSP primaire. Nous commencerons par étudier la répartition du choix des liens par type de trafic et l'impact de la différenciation de trafic sur le choix des liens du LSP primaire. Ensuite, nous ferons une étude statistique sur les probabilités de panne des LSP par classe de résilience et nous terminerons avec l'analyse du taux de succès des deux approches évaluées, en terme de respect de la classification des classes.

La répartition du choix des liens par type de trafic

En faisant une analyse de la répartition des liens par classe de résilience, notre objectif est d'analyser le comportement des deux approches et surtout de valider l'approche DHIRQ. En effet, le choix des liens influence grandement la probabilité de panne du LSP primaire. Le choix des liens par où passe le LSP primaire doit prendre en considération la classification de trafic adoptée dans notre approche DHIRQ et ceci, en favorisant les classes exigeant une bonne résilience et en défavorisant les classe moins exigeantes en terme de résilience. Comme détaillé au Chapitre 3, nous considérons cinq types de liens selon le niveau de la protection optique implémentée : *Amelioré, Dedié 1+1, Dedié 1 :1, Partagé* et *Non protegé.* Pour chaque demande de LSP effectuée dans nos tests, nous gardons en mémoire la liste des liens empruntés. Ainsi, en faisant une

étude statistique sur les 4800 demandes de LSP effectuées dans nos sessions d'évaluation de performance pour le protocole CSPF et pour l'approche DHIRQ, nous avons étudié la répartition des liens selon la classe de résilience. Le résultat de cette étude pour le protocole DHIRQ est présenté à la Figure 4.5. La Figure 4.6 illustre les résultats dans le cas du protocole CSPF.

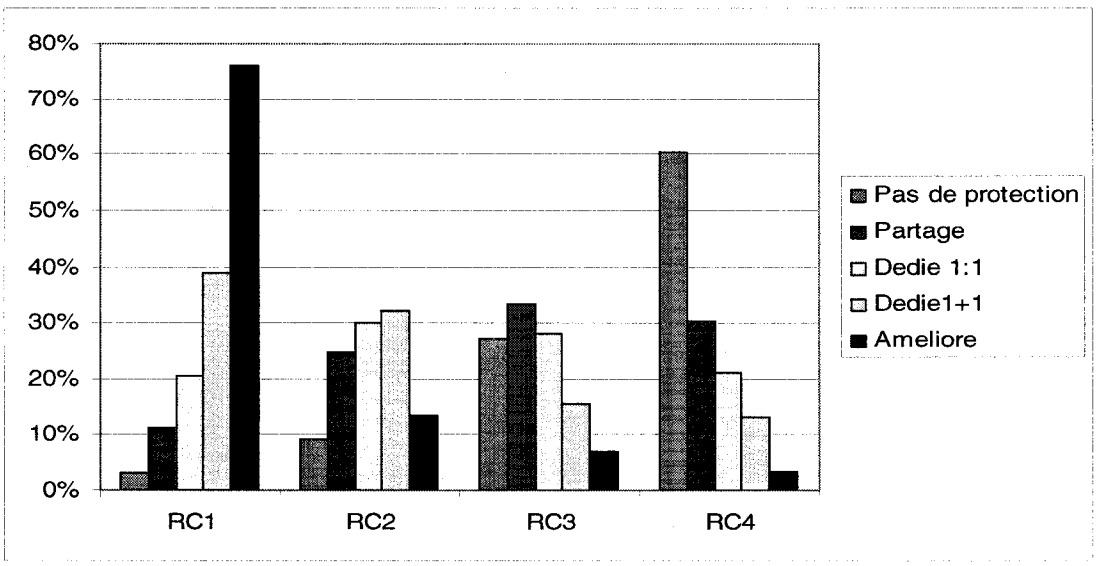

Figure 4.5 Répartition des liens par Classe de résilience avec DHIRQ

Nous remarquons que la répartition des liens par classe de résilience reflète bien les objectifs que nous nous sommes fixés dans le cas de DHIRQ. En effet, 76% des liens de type « amélioré », ayant la meilleure protection optique, ont été utilisés pour transporter du trafic de la classe RC1. La classe RC2 a utilisé 13% de ces mêmes liens. Quant aux classes RC3 et RC4, elles en ont utilisé 7% et 3% respectivement. Pour les liens de type « *dédié 1+1* », la classe RC1 arrive en premier en terme de pourcentage d'utilisation de ce type de liens, avec 39% suivie de la classe RC2 avec 32%. Les classes RC3 et RC4 suivent avec 16% et 13% respectivement. La classe RC2 utilise le maximum de liens de type « *Dédié 1 :1* » avec 30% d'utilisation. Les liens de type « *partagé* » sont plus utilisés par la classe RC3. Quant aux liens « *non protégés* », ils

sont principalement utilisés pour transporter des trafics de la classe RC4 avec un pourcentage de 60%. La répartition des liens pour l'approche DHIRQ reflète bien les attentes théoriques exprimées au Chapitre 3. En effet, nous observons une bonne répartition selon la classification adoptée du trafic. Ainsi, les liens protégés au niveau optique sont réservés prioritairement aux classes de résilience les plus exigeantes.

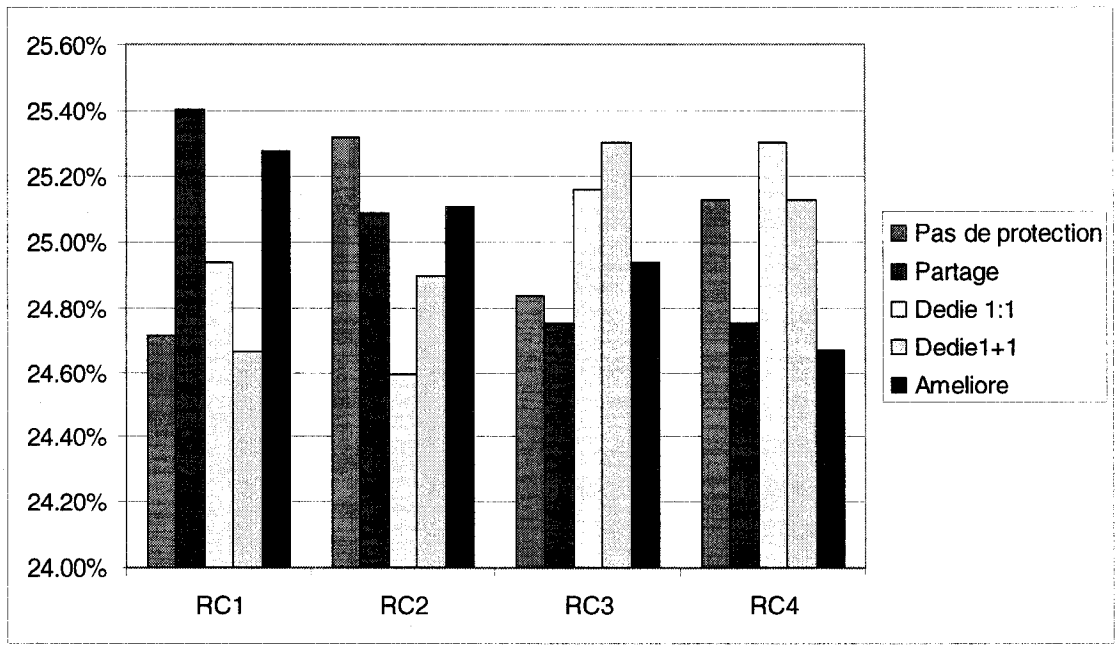

Figure 4.6 Répartition des liens par Classe de résilience avec CSPF

Dans le cas de CSPF, Figure 4.6, nous remarquons que la répartition des liens par classe de résilience est assez équilibrée. En effet, l'utilisation des cinq types de liens est partagée d'une façon égale sur les quatre classes de résilience. Ainsi, une moyenne proche de 25% est observée pour l'ensemble des types de liens. Ceci signifie que le choix des liens n'est pas influencé par la classification de trafic dans le cas de CSPF.

La probabilité de panne des LSPs par classe de résilience

L'objectif principal de l'approche DHIRQ est d'établir des LSP résilients ayant une faible probabilité de panne tout en prenant en considération la classification de

trafic. Dans cette section, nous présentons une étude comparative entre DHIRQ et CSPF en terme de probabilité de panne des LSPs pour les quatre classes de résilience. On considère la moyenne des probabilités de pannes des LSP primaires pour chacune des quatre classes de résilience, soit 1200 LSP par classe. La Figure 4.7 illustre les résultats de cette étude.

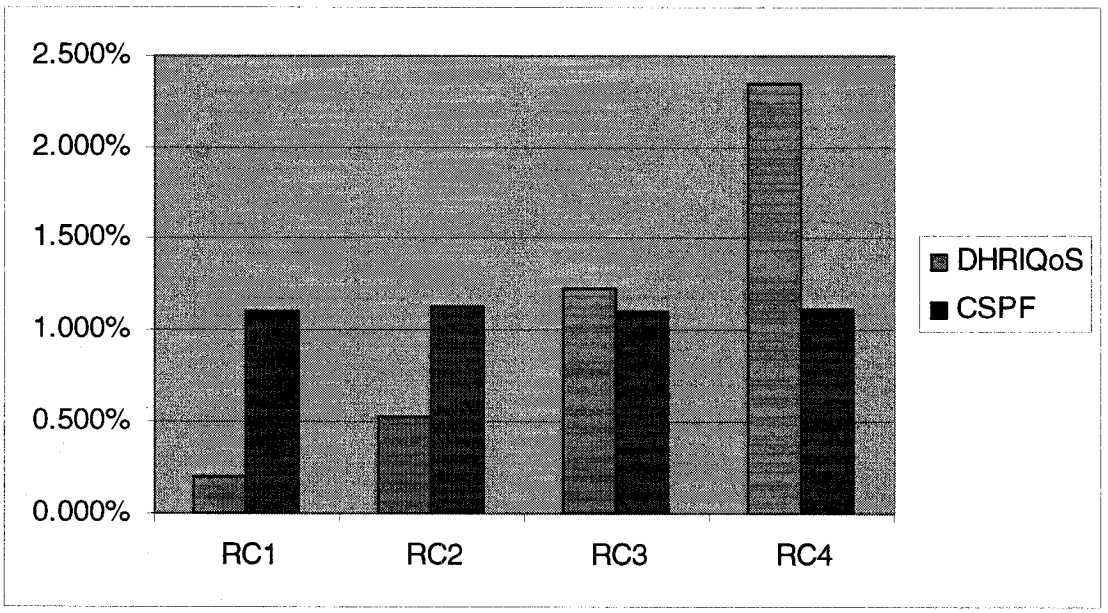

Figure 4.7 Probabilité de panne par classe de résilience

Nous remarquons que DHRIQ offre les probabilités de pannes les plus faibles dans le cas des classes de résilience RC1 et RC2 avec une moyenne de 0.2% et 0.5% respectivement. Les classes RC3 et RC4 présentent des moyennes de panne plus élevées avec DHRIQ qu'avec CSPF. Nous remarquons aussi, dans le cas de DHIRQ, que la probabilité de panne suit bien la classification de trafic adoptée. En effet, la classe de résilience RC1 présente la plus faible moyenne de probabilité de panne, suivie de la classe RC2, de la classe de résilience RC3 et de la classe RC4 avec la plus haute moyenne de probabilité de panne. Le protocole CSPF ne fait pas de distinction entre les différentes classes de résilience et ainsi offre à peu près la même probabilité de panne à l'ensemble des quatre classes.

Analyse du taux de succès

Un des objectifs de notre approche est d'éviter que l'affectation des liens soit liée à l'ordre chronologique des arrivées mais plutôt à la classe de résilience et à la charge des liens. Dans notre évaluation de performance, nous avons étudié l'effet de l'ordre d'arrivée des requêtes et de la charge des liens sur le comportement de notre algorithme. Dans cette section, nous présentons les résultats de l'étude comparative entre DHIRQ et CSPF en terme de respect de la classification des classes de résilience. Le critère de comparaison considéré est la probabilité de panne des LSP primaires. La Figure 4.8 illustre les résultats de cette étude.

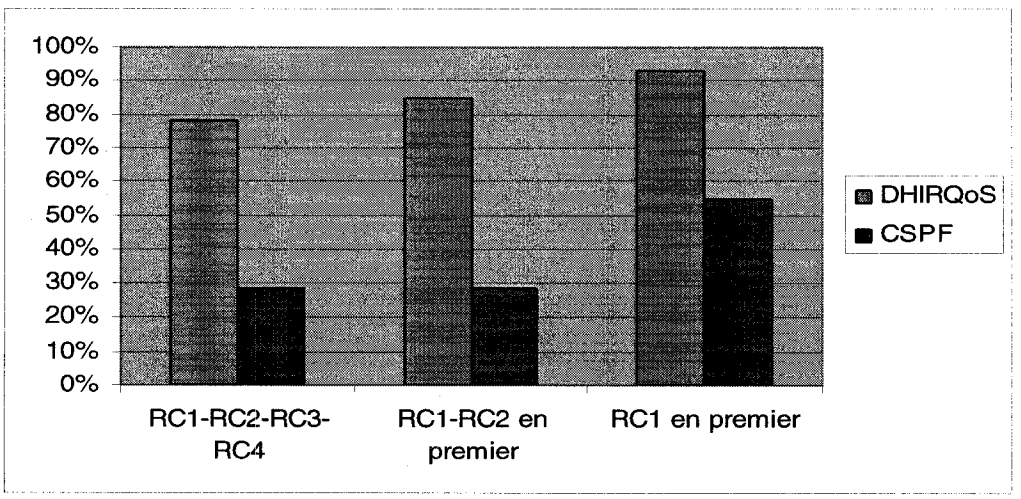

Figure 4.8 Taux de succès CSPF vs DHIRQ

Par taux de succès, nous entendons le pourcentage des tests dans lesquels l'ordre des probabilités de panne par classe de résilience respecte la classification adoptée. En effet, l'ordre idéal croissant des probabilités de panne est : en premier la classe de résilience RC1 avec la plus faible probabilité de panne suivie de RC2, RC3 et RC4. Cet ordre croissant signifie que le LSP de la classe RC1 passe par le chemin le plus résilient en comparaison avec les LSP des autres classes. Suite à notre analyse statistique, nous remarquons que DHIRQ offre de meilleurs résultats par rapport à CSPF en terme de taux

de succès (Figure 4.8). En effet, dans 79% des cas, DHIRQ respecte totalement la classification des classes de résilience contre 28% dans le cas de CSPF. Si nous considérons uniquement la classe de résilience RC1, le taux de succès passe à 92% dans le cas de DHIRQ et à 53% dans le cas de CSPF.

4.4.2 Analyse des résultats de la deuxième phase (Choix des LSP de secours)

Dans cette section, nous analysons les résultats relatifs à la deuxième étape de notre approche qui consiste à protéger le LSP primaire trouvé lors de la première phase de recherche de chemin primaire. Comme détaillé au Chapitre 3, un des objectifs de l'approche DHIRQ est d'optimiser les ressources réseau dédiées à la protection en préconisant le partage des ressources de protection et en favorisant les liens protégés au niveau optique lors du choix des LSP primaires. Dans notre étude de performance, nous avons tenté de vérifier quel est le gain en terme d'utilisation de ressource avec DHIRQ. Nous présenterons en premier les résultats relatifs à la répartition de la protection optique par classe de résilience, puis nous détaillerons quelques exemples illustratifs de la deuxième phase de notre approche.

Répartition de la protection optique par classe

Comme mentionné auparavant, l'approche DHIRQ est une méthode à deux étapes : une première étape de choix de LSP primaire suivie d'une étape de protection du LSP primaire. Lors de la deuxième étape de recherche du LSP de secours, on parcourt le LSP primaire afin de déterminer le lien ou l'ensemble de liens nécessitant une protection globale ou locale dépendamment de la classe de trafic. Seuls les liens non protégés au niveau optique devraient éventuellement être protégés au niveau IP/MPLS. Dans notre évaluation de performance, nous avons étudié le pourcentage des LSP ne nécessitant pas de protection, autrement dit des LSPs dont tous les liens sont protégés au niveau optique. La Figure 4.9 illustre les résultats de cette étude.

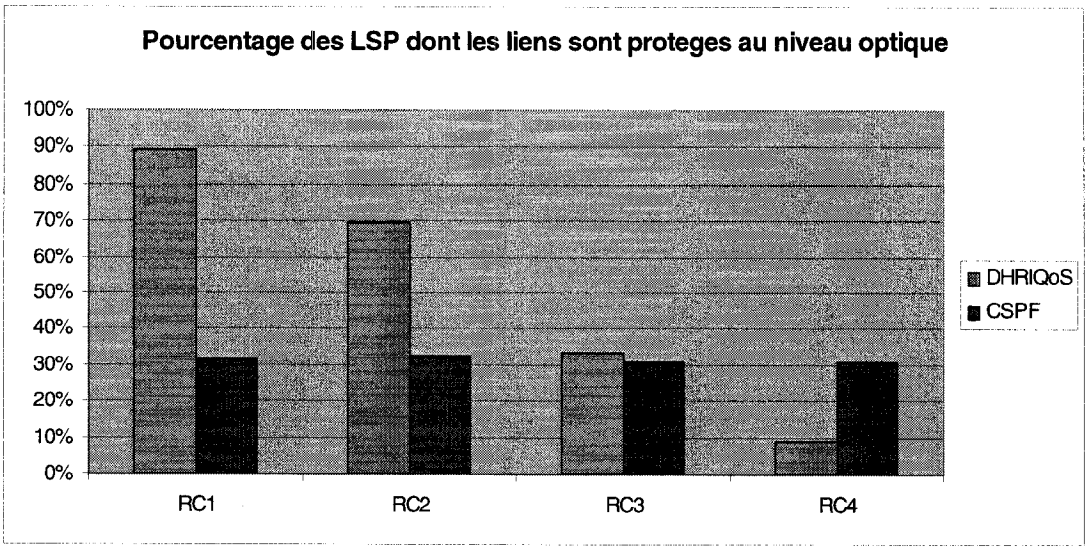

Figure 4.9 Pourcentage des LSPs ne nécessitant pas de protection IP/MPLS

Nous remarquons, dans le cas du protocole DHIRQ, que les LSPs de la classe RC1 arrivent en premier avec presque 90% des LSP ayant l'ensemble de leurs liens protégés au niveau optique. Ceci implique que seul 10% des LSP de la classe RC1 nécessitent une protection à la couche IP/MPLS. Comparé avec CSPF, 32% des LSP de la classe RC1 sont totalement protégés à la couche optique, ce qui implique que 68% des LSPs de cette classe devrait être protégés au niveau IP/MPLS avec des LSP de secours. Ceci montre que le choix du LSP primaire avec la méthode DHIRQ optimise énormément la consommation des ressources de protection et devrait aussi réduire les temps de recouvrement, sachant que la restauration au niveau optique est généralement plus rapide que celle de IP/MPLS. Pour la classe RC2, 70% des LSPs, obtenus avec la méthode DHRIQ, ne nécessitent pas de protection, contre 33% dans le cas de LSP routés avec le protocole CSPF. Nous remarquons aussi, dans le cas de DHIRQ, que la classe RC4 est celle qui a le plus bas pourcentage des LSP totalement protégés au niveau optique. Cela ne pénalise aucunement l'approche DHIRQ sachant que la classe RC4 est réservée aux trafics de moindre importance et qu'aucune protection IP/MPLS est à préconiser dans ce cas.

Exemples illustratifs de la deuxième phase de notre approche

Dans cette section, nous présentons quatre cas en guise d'exemples illustratifs pour montrer le gain en terme de ressource de protection réalisé par l'approche DHIRQ en comparaison avec le protocole CSPF

- Cas 1 : LSP primaire de la classe RC1 avec la méthode DHIRQ

La Figure 4.10 illustre le cas de routage d'un LSP primaire avec la méthode DHIRQ. Le chemin choisi par DHIRQ est le suivant : Nœud Source, Seattle, Utah, Denver, Kansas, Iowa access, Chicago, Detroit, Nœud Destination. Tel que montré au Tableau 4.6, l'ensemble des liens utilisés pour ce LSP primaire sont protégés au niveau optique avec différents niveaux de protection. Ce LSP ne nécessite aucune protection au niveau IP/MPLS avec des LSP de secours, étant donné que tous les liens sont protégés au niveau optique. Ceci implique une réduction dans l'utilisation des ressources destinées à la protection.

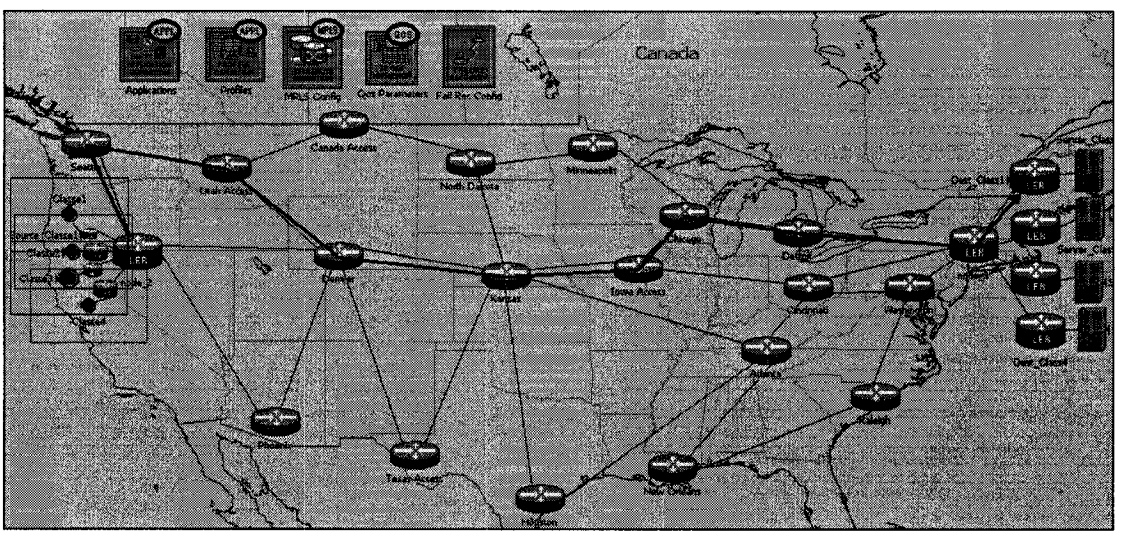

Figure 4.10 LSP primaire de la classe RC1 avec la méthode DHIRQ

Tableau 4.6 Liens du LSP primaire de la classe RC1 avec la méthode DHIRQ

Source	Destination	Protection
NodeSource	Seattle	Dédié 1+1
Seattle	Utah	Dédié 1+1
Utah	Denver	Dédié 1:1
Denver	Kansas	Amélioré
Kansas	Iowa Access	Dédié 1:1
Iowa Access	Chicago	Partagé
Chicago	Detroit	Dédié 1+1
Detroit	NodeDest	Dédié 1+1

- Cas 2 : LSP primaire de la classe RC1 avec la méthode CSPF

Dans ce cas, nous utilisons la même configuration réseau que dans le Cas 1, avec les mêmes protections optiques et probabilités de panne. Nous utilisons le protocole CSPF pour établir le LSP primaire de la classe RC1. La Figure 4.11 illustre ce cas. Le chemin choisi par CSPF est le suivant : Nœud Source, Denver, Kansas, Iowa access, Cincinnati, Nœud Destination. Tel que montre au Tableau 4.7, les deux liens (Nœud Source, Denver) et (Cincinnati, Nœud Destination) ne sont pas protégés à la couche optique et, de ce fait, nécessitent une protection à la couche IP/MPLS. Selon l'approche DHIRQ, la protection locale est à préconiser dans le cas de la classe RC1. Les deux LSP de protection sont montrés à la Figure 4.11. Le premier LSP (Nœud source – Phoenix - Denver) protège le lien (Nœud source - Denver) et le second LSP (Cincinnati – Washington - Nœud Destination) protège le lien (Cincinnati, Nœud Destination). Nous remarquons, en comparant avec le Cas 1, qu'au Cas 2, on a eu recours à deux LSP de secours passant par quatre liens. D'où une plus grande utilisation des capacités réseau pour la protection.

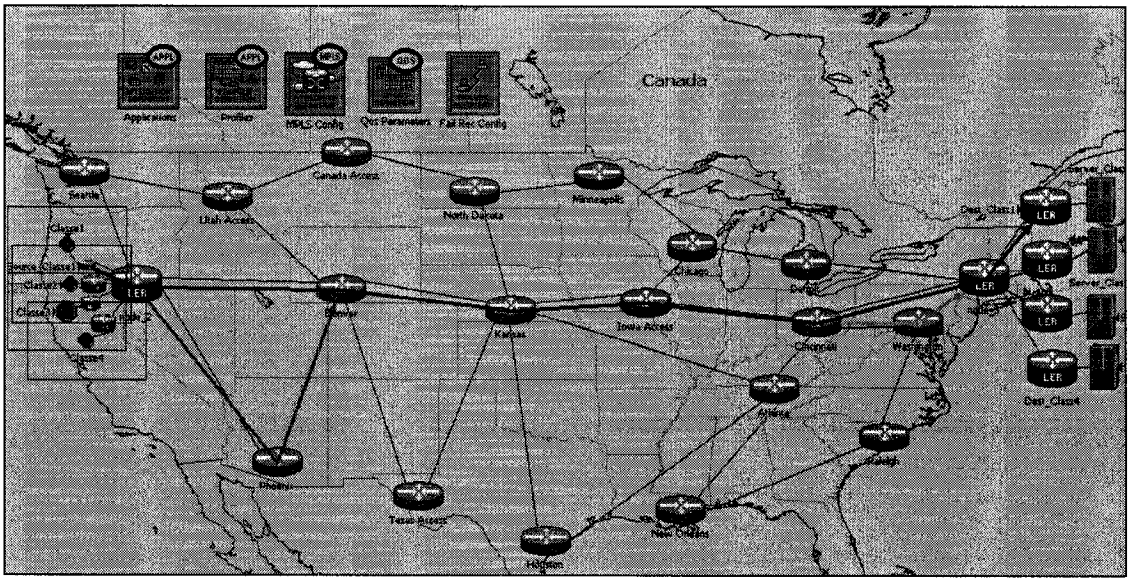

Figure 4.11 LSP primaire de la classe RC1 avec la méthode CSPF

Tableau 4.7 Liens du LSP primaire de la classe RC1 avec la méthode CSPF

Source	Destination	Protection
NodeSource	Denver	Non protégé
Denver	Kansas	Amélioré
Kansas	Iowa Access	Dédié 1:1
Iowa Access	Cincinnati	Partagé
Cincinnati	NodeDest	Non protégé

- Cas 3 : LSP primaire de la classe RC2 avec la méthode DHIRQ

La Figure 4.12 illustre le cas de routage d'un LSP primaire de la classe de résilience RC2 avec la méthode DHIRQ. Le chemin choisi par DHIRQ est le suivant : Nœud source, Phoenix, Denver, Texas, Kansas, Iowa Access, Chicago, Detroit, Nœud destination. Tel que montré au Tableau 4.8, l'ensemble des liens utilisés pour ce LSP primaire sont protégés au niveau optique avec différents niveaux de protection. Ainsi, il

n'est pas nécessaire de protéger ce LSP à la couche IP/MPLS en mettant en place des LSP de secours. D'où un gain en terme d'utilisation des ressources de protection.

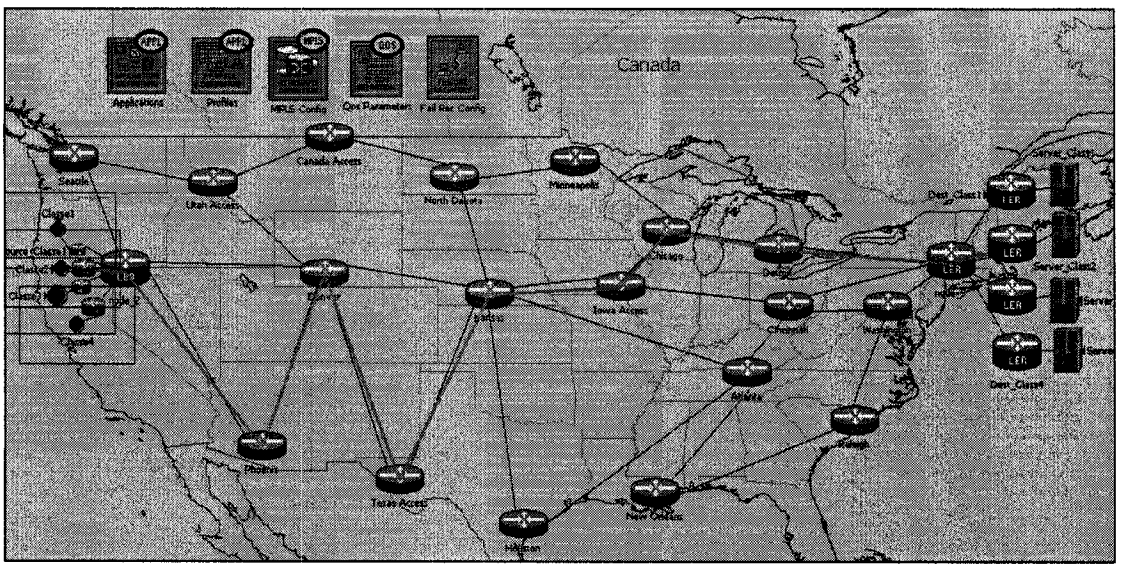

Figure 4.12 LSP primaire de la classe RC2 avec la méthode DHIRQ

Tableau 4.8 Liens du LSP primaire de la classe RC2 avec la méthode DHIRQ

Source	Destination	Protection
NodeSource	Phoenix	Dédié 1:1
Phoenix	Denver	Dédié 1:1
Denver	Texas	Dédié 1+1
Texas	Kansas	Dédié 1:1
Kansas	Iowa Access	Partagé
Iowa Access	Chicago	Dédié 1:1
Chicago	Detroit	Partagé
Detroit	NodeDest	Partagé

- Cas 4 : LSP primaire de la classe RC2 avec la méthode CSPF

Dans ce cas, nous gardons la même configuration des protections optiques et probabilités des pannes que dans le Cas 3. Nous utilisons le protocole CSPF pour établir le LSP primaire de la classe RC2. La Figure 4.13 illustre ce cas. Le chemin choisi par CSPF est le suivant : Nœud Source, Denver, Kansas, Atlanta, Cincinnati, Nœud Destination. Tel que montré au Tableau 4.9, les deux liens (Denver, Kansas) et (Kansas, Atlanta) nécessitent une protection à la couche IP/MPLS, étant donné qu'ils ne sont pas protégés à la couche optique. Selon l'approche DHIRQ, la protection globale/segment est à préconiser dans le cas de la classe RC2. Ainsi, afin de protéger ce LSP primaire, un LSP de secours a été signalé. Ce LSP de secours emprunte le chemin suivant : Denver, Utah access, Canada access, North Dakota, Minneapolis, Chicago, Detroit, Nœud destination. On remarque en comparant avec le Cas 3 qu'au Cas 4, on a eu recours à un LSP de secours passant par sept liens utilisant ainsi plus de ressources de protection que dans le Cas 3.

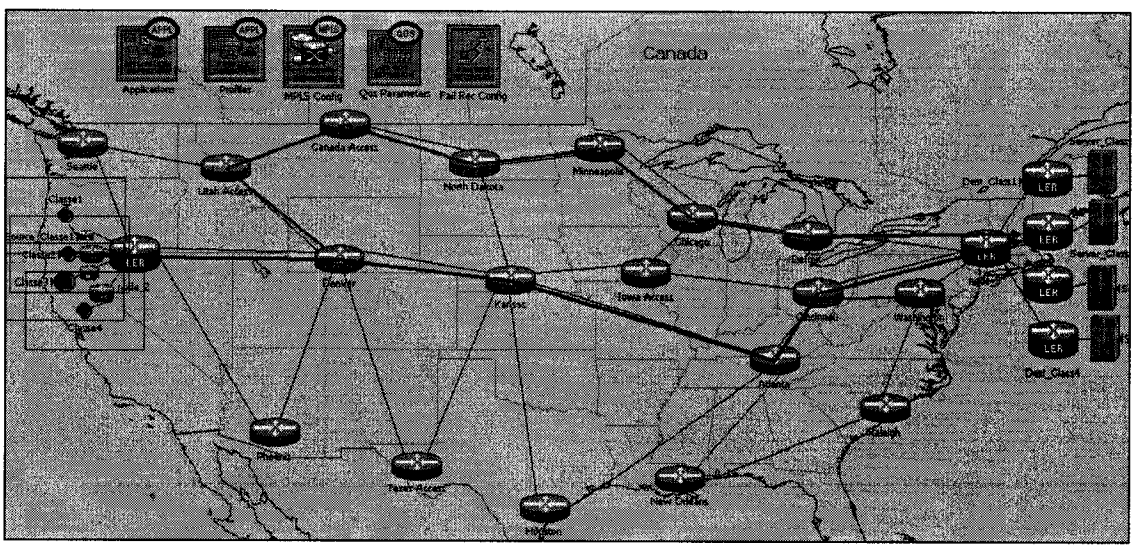

Figure 4.13 LSP primaire de la classe RC2 avec la méthode CSPF

Tableau 4.9 Liens du LSP primaire de la classe RC2 avec la méthode CSPF

Source	Destination	Protection
NodeSource	Denver	Amélioré
Denver	Kansas	Non protégé
Kansas	Atlanta	Non protégé
Atlanta	Cincinnati	Amélioré
Cincinnati	NodeDest	Dédié 1+1

4.5 Discussion et améliorations

Afin d'implémenter tous les aspects de l'approche DHIRQ et ainsi optimiser les résultats et les performances de notre algorithme, plusieurs éléments peuvent être améliorés.

Implémenter l'algorithme sur un outil de simulation ayant un plan de contrôle unifié

L'outil de simulation OPNET Modeler utilisé dans l'évaluation de performance n'implémente pas un plan de contrôle unifié, tel que défini dans le standard GMPLS. OPNET simule un plan de contrôle en couches (*overlay model*) dans lequel la couche IP/MPLS n'a pas une visibilité sur les possibilités de la couche optique en termes de protection et de restauration. Ceci pénalise l'implémentation de notre approche sur l'outil OPNET. En effet, un des aspects de notre approche est d'optimiser le temps de restauration de façon adaptative, en fonction de la disponibilité de la protection optique ou pas sur le lien en panne. La solution proposée préconise de ne pas allouer un temps d'attente *(Hold off time)* dans le cas d'absence de protection optique. L'implémentation d'une telle fonctionnalité s'avère impossible avec la version actuelle d'OPNET. Aussi, les protocoles de routage et de signalisation implémentés dans OPNET ne sont pas de type intégrés et ceci est dû aussi au fait que le plan de contrôle dans OPNET suit un modèle en couches. Ce dernier point pose un problème important qui est l'absence des

protocoles de routage de type intégré déjà implémentés sur OPNET avec lesquels on peut confronter notre approche de routage DHIRQ.

Support de la restauration au niveau optique

Afin de simuler tous les aspects de l'approche DHIRQ dont la simulation de panne, il faut avoir la possibilité d'implémenter les différents types de protection optique sur l'outil de simulation et de disposer d'un plan de contrôle unifié pour faire interagir la couche optique avec les mécanismes de protection IP/MPLS. Pour le moment, l'outil de simulation OPNET se limite à l'implémentation de scénarios de panne au niveau IP/MPLS uniquement.

Définition dynamique des LSPs

Un autre aspect caractéristique de l'approche DHIRQ est la définition dynamique des LSPs primaires et de secours. Malheureusement, la définition des LSPs dynamiques sur l'outil OPNET impose la désignation au moins de la source et de la destination lors de la définition du modèle et bien avant le début des simulations. Or, dans notre approche, le choix des LSP de secours se fait dans la deuxième étape de l'algorithme, à savoir après la définition du LSP primaire. Cela implique que la connaissance préalable de la source et destination du LSP de secours avant le début des simulations est impossible.

CHAPITRE V
CONCLUSION

5.1 Synthèse des travaux

Notre travail de recherche a porté sur la survivabilité des réseaux dorsaux GMPLS. Nous avons proposé une nouvelle approche de routage dynamique des LSPs, qui tire profit du plan unifié de GMPLS et qui assure un niveau de résilience adéquat au type de trafic transporté. L'algorithme proposé présente les caractéristiques et avantages suivants :

- *Dynamique* : Il assure l'approvisionnement des LSPs primaires et secondaires de façon dynamique, indépendamment de l'ordre chronologique des arrivées des requêtes;
- *Intégré* : Il prend en considération les mécanismes de protection disponibles dans la couche optique lors du choix des chemins des LSPs;
- *Adaptatif et hybride* : Il assure une différenciation de service, selon la classification de trafic adoptée, lors du choix du LSP primaire et de la méthode de protection;
- *Efficace* : Il optimise l'utilisation des ressources réseau destinées à la protection en choisissant de façon judicieuse les LSP primaires.

Afin d'évaluer la performance de notre proposition, l'algorithme a été implémenté sur OPNET Modeler et plusieurs sessions de simulation ont été faites pour différentes valeurs des facteurs choisis dans notre plan d'expérience. Les résultats de l'évaluation des performances de DHIRQ en comparaison avec CSPF, tous deux implémentés dans OPNET Modeler, montre que notre approche offre de meilleurs résultats en terme de probabilité de pannes des LSP primaires et une meilleure utilisation des ressources de protection.

5.2 Limitation des travaux

La problématique de la résilience des réseaux informatiques peut être abordée de plusieurs manières : faire une supervision en temps réel du comportement du réseau et de ses performances, implanter des solutions redondantes, prévoir des chemins de secours pré-réservés pour faire face aux pannes ou encore implémenter des mécanismes réactifs qui vont réagir après la panne. Généralement, les solutions implantées en pratique sont un amalgame de plus d'une solution parmi celles citées ci-haut. Dans ce mémoire, nous nous sommes penché sur les mécanismes de protection qui consistent à réserver au préalable des chemins de secours. Nous avons aussi émis plusieurs hypothèses simplificatrices. Une des hypothèses émises est que le réseau dispose d'un mécanisme de signalisation qui permet à tous les nœuds d'avoir un ensemble d'informations sur les liens auxquels ils sont attachés. En effet, nous avons supposé que chaque nœud a accès aux informations sur les capacités en bande passante et le niveau de la protection optique de chacun des liens. Une telle hypothèse nécessiterait que le protocole de réservation, en l'occurrence RSVP-TE, soit modifié afin d'inclure les informations sur la bande passante et la protection optique dans les messages de signalisation. Une deuxième hypothèse émise lors de la conception de l'algorithme est que juste une seule panne de lien se produit dans le réseau. Une amélioration qui peut être apportée à notre algorithme est la prise en charge des pannes multiples et des pannes de nœuds. Pour la prise en considération des pannes de nœuds, une solution intuitive serait d'associer des probabilités de pannes aux nœuds du réseau et de considérer ces probabilités lors du choix des chemins primaires et de secours. Ainsi, le passage par des nœuds, ayant une haute probabilité de panne, serait évité dans le cas d'une classe à haute exigence en terme de résilience telle que la classe RC1.

5.3 Orientations de recherche future

Différentes améliorations peuvent être apportées à la solution proposée, ce qui pourrait constituer des orientations pour de futurs travaux de recherche. Dans l'approche DHIRQ, nous considérons que chaque nœud dispose des informations sur les capacités

en bande passante et du niveau de la protection optique de chacun des liens auxquels il est connecté. Ces informations sont supposées être disponibles grâce à un protocole de signalisation. Ainsi, une orientation de recherche serait de mettre en place un tel mécanisme de signalisation ou d'améliorer un protocole existant tel que RSVP-TE pour supporter ces nouvelles fonctionnalités. Une autre possibilité de recherche serait de modifier l'algorithme proposé afin d'effectuer la recherche du LSP primaire et de secours de façon parallèle, au lieu d'effectuer deux étapes de recherche de LSP tel que proposé. L'idée derrière cela est que le fait de chercher une paire de LSP (LSP primaire et LSP de secours) en même temps pourrait permettre d'optimiser globalement l'utilisation des ressources réseau. Dans ce cas, l'objectif de l'algorithme serait de trouver une paire de LSPs qui utilise le moins de ressources et qui offre le niveau de résilience exigée par la classe de trafic. Une autre possibilité d'amélioration serait d'étudier la stabilité de notre algorithme en cas de panne. En effet, notre approche se base, en partie, sur les informations de disponibilité de la bande passante pour calculer les chemins résilients et optimaux. Cette information change dynamiquement et peut être affectée en cas de panne. Cela peut mener à une situation où les informations sur la disponibilité de la bande passante, contenues dans les nœuds, ne reflètent pas l'état réel du réseau ce qui, par conséquent, pourrait affecter les résultats de notre algorithme. Une telle étude d'amélioration consisterait donc à étudier le comportement de notre proposition en cas de panne et d'analyser la stabilité de l'algorithme. Une autre voie d'amélioration serait de supporter des pannes multiples et des pannes de nœuds.

BIBLIOGRAPHIE

ANDERSSON, L., Doolan, P., Feldman, N., Fredette, A., Thomas, B., "LDP specification". IETF RFC 3036, January 2001.

AUTENRIETH, A., KIRSTÄDTER, A., "Engineering End-to-End IP Resilience Using *Resilience-Differentiated QoS*", IEEE Communications Magazine, Vol. 40, No. 1, Jan 2002, pp. 50-57.

AWDUCHE, D., BERGER, L., GAN, D., LI, T., SRINIVASAN, V., SWALLOW, G., "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

BERGER, L., Editor, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description", RFC 3471, January 2003.

BERGER, L., Editor, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

BRADEN, R., ZHANG, L., BERSON, S., HERZOG, S., JAMIN S.. "Resource ReSerVation Protocol (RSVP)". IETF RFC 2205, September 1997.

CALLE, E., "Enhanced fault recovery methods for protected traffic services in GMPLS networks", Thèse de doctorat (PhD.), département d'informatique, d'automatique et d'électronique, Université de Girona, Février 2004.

DAVIE, B., REKHTER, Y., "MPLS Technology and Applications". Morgan kaufmann publisher Inc. ISBN 1-55860-656-4, May 2000.

DEMEESTER, P., AUTENRIETH, A., BRIANZA, C., CASTAGNA, L., SIGNORELLI, G., CLEMENTE, R., RAVERA, M., JAJSZCZYK, A., JANUKOWICZ, D., VAN DOORSELAERE, K., HARADA, Y.",Resi*lience in Multilayer Networks*", IEEE Communications Magazine, August 1999.

FUMAGALLI, A., VALCARENGHI, L., "IP Restoration vs. WDM Protection*: Is There an* Optimal Choice?", IEEE Networks, Vol. 14, No. 6, Nov-Dec 2000, pp. 34–41.

HUANG, C., SHARMA,V., OWENS, K., MAKAM, S., "Building reliable MPLS Networks using *a path protection mechanism*", IEEE Communications Magazine, Vol 40, No 3, March 2002, pp. 156–162.

KOMPELLA, K., REKHTER, Y., Editors, "IS-IS Extensions in Support of Generalized MPLS", Internet Draft, December 2002.

KOMPELLA, K., REKHTER, Y., Editors, "OSPF Extensions in Support of Generalized MPLS", Internet Draft, October 2003.

LANG, J., editor, "Link Management Protocol", Internet Draft, October 2003.

MANNIE, E., Editor, "Generalized Multi-Protocol Label Switching Architecture", Internet Draft, May 2003.

MANNIE, E., PAPADIMITRIOU, D., "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)", Internet Draft, April 2004.

MARZO, J., CALLE, E., SCOGLIO, C., ANJALI, T., "QoS On-Line Routing and MPLS Mu*ltilevel Protection: a Survey*", IEEE Communications Magazine, Vol 41, No 10, Oct 2003, pp. 126–132.

MOY, J., "OSPF Version 2", IETF RFC 2328, April 1998.

ORAN, D., "IS-IS Intra-domain Routing Protocol" RFC 1142, February 1990.

PAPADIMITRIOU, D., JONES, J., BASAK, D., HARTANI, R., "Packet-Optical Escalation Strategies—Framework", Internet Draft, May 2002.

PEPELNJAK, I., GUICHARD, J., "MPLS and VPN Architectures". Pearson Education Canada. ISBN 1-58705-002-1, October 2000.

PONGPAIBOOL, P., "Survivability of GMPLS-based IP-over-optical networks", Thèse de doctorat (PhD.), département du génie informatique et électrique, Université de Carnegie Mellon, Mai 2004.

ROSEN, E., VISWANATHAN, A., CALLON, R., "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

SHARMA, V., CRANE, B., MAKAM, S., OWENS, K., HUANG, C., HELLSTRAND, F., WEIL, J., ANDERSSON, L., JAMOUSSI, B., CAIN, B., CIVANLAR, S., CHIU, A., "Framework for MPLS-Based Recovery". RFC3469. February 2003.